ANNALES SCIENTIFIQUES DE L'É.N.S.

ALBERT CHÂTELET

Arithmétique des corps abéliens du troisième degré

Annales scientifiques de l'É.N.S. 3e série, tome 63 (1946), p. 109-160

<http://www.numdam.org/item?id=ASENS_1946_3_63__109_0>

ARITHMÉTIQUE DES CORPS ABÉLIENS

DU TROISIÈME DEGRÉ

PAR M. ALBERT CHATELET.

Depuis D. Hilbert, la théorie des corps de nombres algébriques s'est développée surtout autour de la théorie du corps des classes et des lois de réciprocité (ainsi qu'il est exposé dans le fascicule 75 du *Mémorial des Sc. Math.* rédigé par J. Herbrand et complété par G. Chevalley). La théorie du corps des classes se propose d'étudier comment se décompose un idéal d'un corps donné k dans une extension abélienne K, également donnée. Les lois de réciprocité tendent à mettre sous la forme la plus simple et la plus maniable les critères de décomposition.

Si le présent Mémoire se termine par un résultat qui n'est qu'un cas particulier des lois de réciprocité, il n'en étudie pas moins, au préalable, un problème différent. Les successeurs de D. Hilbert ont considéré que l'extension abélienne K était connue en même temps que le corps de base k, et ils ne se sont pas toujours préoccupés de la façon dont on pouvait construire effectivement cette extension. Cette construction n'est cependant pas un problème trivial : il apparaît simple d'obtenir une équation dans un corps et d'introduire toutes ses racines de façon à obtenir une extension galoisienne, on ne sait pas *a priori* si cette extension est abélienne. On peut tenter de résoudre ce premier problème en utilisant la résolvante de Lagrange et en utilisant au lieu de k une première extension par addition de certaines racines de l'unité. Mais d'autre part on peut aussi chercher un corps qui contienne K et qui soit de définition ou de construction plus simple.

Ce sont ces deux procédés qui, dans ce Mémoire, sont appliqués à la construction des extensions abéliennes, appelées $\mathbf{R}_\theta$ (au lieu de K) du troisième degré, relatives au corps $\mathcal{R}$ des rationnels (pris pour corps de base k). Les deux procédés, même dans ce cas particulier, ne sont pas nouveaux; le premier a été exposé succinctement dans *l'Algèbre* de H. Weber (t. II, chap. IV); le deuxième n'est autre qu'une utilisation des *périodes* introduites par Gauss dans l'étude des racines de l'unité et déjà entrevues avant lui (d'après une indication que m'a donnée M. H. Lebesgue) par Van der Monde. Par ailleurs on sait que Kronecker avait affirmé que tout corps abélien (relativement au corps $\mathcal{R}$ des rationnels) est sous-corps d'un corps circulaire, et cette affirmation a été démontrée par H. Weber (*Algèbre*, t. II, chap. XXII), puis par D. Hilbert (*Théorie des corps de nombres algébriques*, chap. XXIII).

Mais une étude plus précise de cette double génération, au moins dans le cas d'un corps $\mathbf{R}_\theta$ permet d'étudier les *entiers* et les *idéaux* de ce corps. Elle permet aussi de distinguer parmi les corps $\mathbf{R}_\theta$, certains d'entre eux particulièrement simples (ou *primaires*) dont les *discriminants* sont des puissances de certains nombres premiers (4^e puissance de 3 ou carré de tout nombre premier, mult. $3+1$); les autres corps se déduisent de ceux-là par un procédé de composition (ou de multiplication). Enfin la comparaison des deux modes de génération donne une preuve particulièrement intuitive, dans le cas considéré, de la *loi de réciprocité*; elle précise quels sont les nombres premiers (appartenant à des progressions arithmétiques déterminées) qui se décomposent dans un corps connu $\mathbf{R}_\theta$; cette preuve évite notamment l'introduction de tout élément transcendant.

Les raisonnements et les résultats ainsi exposés pour les corps du troisième degré sont susceptibles de généralisation pour les corps abéliens de degré quelconque. Pour amorcer cette généralisation, j'ai indiqué comment chaque paragraphe pouvait être traité de façon analogue pour les corps quadratiques; j'ai précisé notamment la composition, rarement signalée, de tous les corps quadratiques au moyen de corps primaires, dont les discriminants sont ou les nombres premiers de signe convenable [$+$(mult. $4+1$); $-$(mult. $4-1$)], ou l'un des nombres -4, $+8$, -8. Je rappelle de même la démonstration connue de la *loi de réciprocité quadratique* par la considération du corps circulaire qui contient le corps quadratique, démonstration qui, à mon avis, est plus naturelle que les démonstrations dites directes ou élémentaires.

Pour la bibliographie je renvoie au Rapport de D. Hilbert et au fascicule de J. Herbrand cités ci-dessus. Je me contente de signaler que certains des résultats de ce Mémoire ont été indiqués de façon succincte dans des Notes déjà anciennes aux *Comptes rendus de l'Académie des Sciences* (mai 1911, mars et oct. 1920) et dans une communication au Congrès des Mathématiciens de Strasbourg (1921); à ce même Congrès avait été exposé l'un des premiers travaux de T. Takagi sur la théorie du corps des classes.

I. — Corps des racines cubiques de l'unité.

1. Je désigne, suivant une notation courante, les *racines cubiques de l'unité* par les lettres

$$j = -\frac{1}{2} + \frac{i}{2}\sqrt{3}, \qquad j' = -\frac{1}{2} - \frac{i}{2}\sqrt{3}.$$

Dans le *corps quadratique* $\mathbf{R}_j = \mathbf{R}_{j'}$, engendré par ces racines, les couples d'entiers (algébriques) conjugués sont les nombres, mis sous *formes canoniques*

$$\alpha = aj + a'j', \qquad \alpha' = aj' + a'j;$$

où a et a' sont des entiers ordinaires (rationnels). Ils constituent un *anneau* $\mathbf{E}_j$, qui contient les entiers rationnels donnés par

$$a = a' = -m; \qquad \alpha = \alpha' = m.$$

Les autres nombres du corps sont les quotients de ceux-là par des entiers rationnels positifs (supérieurs à 1, et premiers avec le p. g. c. d. de a, a').

La transposition de j et j' fait correspondre à chaque nombre α (entier ou non) du corps, son conjugué α' (représenté par la même lettre accentuée); elle définit un *automorphisme* à la fois pour le corps $\mathbf{R}_j$ et pour l'anneau $\mathbf{E}_j$; le carré de cet automorphisme est la transformation identique.

2. Je rappelle les propriétés de *divisibilité* de l'anneau $\mathbf{E}_j$. Il contient 6 *diviseurs de l'unité* (dont les inverses sont entiers)

$$\varepsilon = \pm 1, \quad \text{ou} \quad \pm j, \quad \text{ou} \quad \pm j'.$$

Ses *nombres premiers* sont donnés par les règles suivantes :

a. Tout entier (rationnel positif) *premier q, congru à* -1 (*mod* 3), *est indécomposable*, ses produits εq par les 6 diviseurs de 1 (appelés associés) sont des *nombres premiers dans* $\mathbf{E}_j$. Leur *norme* commune est q^2 (ils sont dits pour cette raison, du *second degré*).

b. Tout entier (rationnel positif) *premier p, congru à* $+1$ (*mod* 3), *est décomposable en un produit de deux entiers conjugués différents*

$$p = \varpi\varpi' = (aj + a'j')(aj' + a'j); \qquad (\varpi \neq \varepsilon\varpi').$$

Les produits $\varepsilon\varpi$ et $\varepsilon\varpi'$, de chacun d'eux par les six diviseurs de 1, sont des *nombres premiers* (associés) *dans* $\mathbf{E}_j$. Leur *norme* commune est p (ils sont dits du *premier degré*).

c. L'entier 3 *est,* au produit près par un diviseur ε de 1, *le carré d'un entier* (produit de deux facteurs égaux)

$$3 = -(j - j')^2 = \varepsilon\,\varpi_3^2.$$

Les produits de ce nombre par les 6 diviseurs de l'unité sont des *nombres premiers* (associés) *dans* $\mathbf{E}_j$. Leur *norme* commune est 3 (ils sont encore du *premier degré*, mais, au point de vue de la divisibilité, ils ne sont pas distincts de leurs conjugués).

Il n'y a pas d'autres nombres premiers dans le corps que ceux qui viennent d'être énumérés, et en outre, *tout nombre (entier) de* $\mathbf{E}_j$ *est décomposable d'une et d'une seule façon,* au produit près par des diviseurs de 1, *en un produit de nombres premiers.* Son conjugué est le produit des conjugués; sa norme est le produit des normes

$$\alpha = \varepsilon \, \Pi \varpi_i^{a_i} \, \Pi q_j^{b_j}; \qquad \alpha' = \varepsilon' \, \Pi \varpi_i'^{a_i} \, \Pi q_j^{b_j};$$
$$\mathrm{N}(\alpha) = \mathrm{N}(\alpha') = \Pi p_i^{a_i} \, \Pi q_j^{2b_j}; \qquad [p_i = \mathrm{N}(\varpi)_i];$$

(i, j, indices entiers; a_i, b_j exposants entiers rationnels positifs).

Le théorème de Lejeune-Dirichlet sur la progression arithmétique, ou un raisonnement direct sur les facteurs premiers du nombre $\mathrm{N}^2 + \mathrm{N} + 1$ (où N est le produit des premiers nombres premiers) montre qu'il y a une infinité de nombres premiers de chacun des degrés).

3. La définition des *congruences* et des *classes,* suivant un module entier μ, est valable dans $\mathbf{E}_j$; le nombre des classes est la norme de ce module; ces classes forment un *anneau,* qui est un *corps,* dans le cas où le module est premier. Dans tous les cas l'ensemble des classes, premières avec le module, constitue un groupe abélien, qui peut être construit par les produits des puissances d'un certain nombre de générateurs

$$\alpha \equiv \gamma_1^{a_1} \gamma_2^{a_2} \ldots, \quad (\mathrm{mod}\ \mu); \qquad [a_1 \ \mathrm{mod}\ d_1;\ a_2 \ \mathrm{mod}\ d_2;\ \ldots];$$

le système des a_i est l'*indice multiple* de α, relativement à la base $\gamma_1, \gamma_2, \ldots$. Je précise ces propriétés dans quelques cas.

a. Pour un *module premier* q *du second degré,* de norme q^2 (q congru à -1, mod 3), les classes peuvent être définies par les représentants

$$aj + a'j'; \qquad [a,\ a' \text{ entiers rationnels, définis mod } q].$$

Les classes non nulles forment un groupe cyclique $\mathbf{G}_{(q)}$, engendré par les puissances d'une certaine classe, à représentant γ non rationnel

$$\gamma^x, \quad (\mathrm{mod}\ q); \qquad [x \text{ défini mod } (q^2 - 1)].$$

Elles comprennent $q - 1$ classes à représentant rationnel ($a \equiv a'$, mod q) obtenues par les $q - 1$ puissances de γ, d'exposants multiples de $q + 1$.

b. Pour un *module premier* ϖ *du premier degré,* de norme p (p congru à $+1$, mod 3), les classes peuvent être définies par des représentants rationnels (définis, mod p). Les classes non nulles forment un groupe cyclique $\mathbf{G}_{(p)}$, isomorphe au groupe des classes non nulles, mod p, dans le corps $\mathcal{R}$ des rationnels; elles sont définies par les mêmes représentants

$$g^x, \quad (\mathrm{mod}\ \varpi); \qquad [x \text{ défini mod } (p - 1)].$$

Suivant le *module composé* $p=\varpi\varpi'$, il y a p^2 classes, dont $(p-1)^2$ premières avec p, qui constituent un groupe multiplicatif abélien qui peut être défini par 2 *générateurs conjugués*

$$\gamma^{x}\gamma'^{x'};\qquad \left\{\begin{array}{l} \qquad\qquad x, x' \text{ définis mod } (p-1);\\ \gamma\left\{\begin{array}{ll}\equiv +1, & (\text{mod } \varpi'),\\ \equiv g, & (\text{mod } \varpi);\end{array}\right. \quad \gamma'\left\{\begin{array}{ll}\equiv +1, & (\text{mod } \varpi),\\ \equiv g, & (\text{mod } \varpi').\end{array}\right.\end{array}\right.$$

c. Pour le *module premier* $(j-j')$, du premier degré, de norme 3 il y a 3 classes caractérisées par les représentants $0, +1, -1$.

Suivant le module $3=-(j-j')^2$, il y a 9 classes, dont 6 premières avec le module, constituant un groupe abélien qui peut être défini par 2 *générateurs*

$$(-1)^x j^y,\quad (\text{mod } 3);\qquad (x, \text{ mod } 2;\quad y, \text{ mod } 3).$$

Suivant le module $9=(j-j')^4$, il y a $9\times 6=54$ classes premières avec le module, elles constituent un groupe abélien qui peut être défini par 3 générateurs

$$2^x(3j+4j')^y(2j-j')^z,\quad (\text{mod } 9);\qquad (x, \text{ mod } 6;\ y \text{ et } z, \text{ mod } 3).$$

4. Pour la construction des corps abéliens, de degré 3, j'aurai à considérer plus spécialement des couples de $\mathbf{E}_j$, que j'appelle *canoniques* et qui sont définis par les conditions de divisibilité suivantes.

Un couple canonique, et par suite son conjugué, *est un système de deux entiers conjugués, premiers entre eux :*

$$\|\alpha\quad \alpha'\|,\qquad \text{ou}\qquad \|\alpha'\quad \alpha\|;\qquad [\alpha, \alpha' \in \mathbf{E}_j;\qquad \text{p. g. c. d.}\,(\alpha, \alpha')=1];$$

et dont l'un d'eux, et par suite aussi l'autre, *est sans facteur carré.*

Cette définition peut être remplacée par la propriété caractéristique :

Un couple de deux entiers conjugués est canonique, *si l'un d'eux,* et par suite aussi l'autre, *est sans facteur rationnel, sans facteur commun avec* 3 *et sans facteur carré.*

Le p. g. c. d. de deux entiers conjugués (α, α') est égal à son conjugué ; il est donc équivalent de dire qu'il est différent de 1 (contradictoire de la 1re partie de la définition) ou qu'il contient soit un facteur rationnel, soit un facteur commun avec 3 (contradictoire de la partie correspondante de la propriété caractéristique). La décomposition d'un nombre premier rationnel p, congru à $+1$, (mod 3), donne notamment deux nombres d'un couple canonique.

A un couple canonique sont *associés* (nombres égaux au produit près par ε) 12 *couples canoniques différents*

$$\left\{\begin{array}{l}\pm\|\alpha\quad \alpha'\|,\\ \pm\|\alpha'\quad \alpha\|,\end{array}\right.\qquad \left\{\begin{array}{l}\pm\|j\alpha\quad j'\alpha'\|,\\ \pm\|j'\alpha'\quad j\alpha\|,\end{array}\right.\qquad \left\{\begin{array}{l}\pm\|j'\alpha\quad j\alpha'\|,\\ \pm\|j\alpha'\quad j'\alpha\|.\end{array}\right.$$

Ces couples sont ainsi répartis en 3 quadruples contenant chacun 2 paires opposées de couples conjugués.

5. Pour distinguer entre ces six paires associées de couples conjugués, je considère les 6 classes de $\mathbf{E}_j$, suivant le module 3, premières avec 3. Le nombre α étant premier avec 3, ses produits par les 6 classes sont respectivement congrus, à l'ordre près, aux 6 classes elles-mêmes; et l'un d'eux est congru à $+1$.

Une notation convenable permet donc d'écrire les 6 paires associées, représentées chacune par un seul des couples conjugués :

$$\left\{\begin{matrix} \pm\|\alpha \quad \alpha'\|, \\ \alpha\equiv\alpha'\equiv+1, \end{matrix}\right. \qquad \left\{\begin{matrix} \pm\|\alpha j, & \alpha' j'\|, \\ \alpha j\equiv j, & \alpha' j'\equiv j', \end{matrix}\right. \qquad \left\{\begin{matrix} \pm\|\alpha j', & \alpha' j\|, \\ \alpha j'\equiv j', & \alpha' j\equiv j, \end{matrix}\right. \qquad (\text{mod } 3).$$

Je dirai qu'*un couple* (canonique) *est*, ainsi que son conjugué, *unitaire, positif ou négatif, lorsque ses nombres sont congrus tous deux, à* $+1$ *ou à* -1 (premier quadruple). Les coefficients de j, j' dans les formes canoniques, sont alors congrus à -1 ou à $+1$.

Exceptionnellement la décomposition du nombre 1 (produit jj') peut être considérée comme définissant seulement 2 paires conjuguées de couples canoniques (opposés) non unitaires

$$\pm\|j \quad j'\|, \qquad \pm\|j' \quad j\|.$$

6. Deux couples sont *premiers entre eux* lorsque chaque nombre de l'un est premier avec chaque nombre de l'autre. Il en est alors de même de tout couple associé à l'un avec tout couple associé à l'autre, en particulier des couples conjugués et opposés. Il est équivalent que *les normes soient premières entre elles*.

Le produit de deux couples est le couple obtenu en formant les produits respectifs des nombres de même rang :

$$\|\alpha_1 \quad \alpha'_1\|\times\|\alpha_2 \quad \alpha'_2\|=\|\alpha_1\alpha_2 \quad \alpha'_1\alpha'_2\|.$$

Les produits des couples conjugués de deux paires

$$(\|\alpha_1 \quad \alpha'_1\| \quad \text{ou} \quad \|\alpha'_1 \quad \alpha_1\|) \quad \text{et} \quad (\|\alpha_2 \quad \alpha'_2\| \quad \text{ou} \quad \|\alpha'_2 \quad \alpha_2\|);$$

donnent deux paires de couples conjugués

$$(\|\alpha_1\alpha_2 \quad \alpha'_1\alpha'_2\| \quad \text{ou} \quad \|\alpha'_1\alpha'_2 \quad \alpha_1\alpha_2\|)$$

et

$$(\|\alpha_1\alpha'_2 \quad \alpha'_1\alpha_2\| \quad \text{ou} \quad \|\alpha'_1\alpha_2 \quad \alpha_1\alpha'_2\|).$$

Si les composants sont canoniques et premiers entre eux, ces 4 produits sont aussi canoniques.

Les nombres de chaque couple étant premiers entre eux et premiers avec les nombres de l'autre couple, les produits $\alpha_1\alpha_2$ et $\alpha'_1\alpha'_2$ d'une part, $\alpha_1\alpha'_2$ et $\alpha'_1\alpha_2$ d'autre part sont premiers entre eux. En outre chacun de ces produits ne peut avoir de facteur carré, car tout facteur premier ne peut figurer qu'une seule fois dans un seul des nombres considérés d'abord.

Le remplacement d'un composant par son opposé remplace les produits par leurs opposés. La norme d'un produit est égale au produit des normes des facteurs.

Si les composants sont unitaires, les produits sont unitaires, le signe étant donné par la règle des signes. Par exemple

$$\alpha_1 \equiv \alpha'_1 \equiv \alpha_2 \equiv \alpha'_2 \equiv +1,$$

entraine

$$\alpha_1\alpha_2 \equiv \alpha'_1\alpha'_2 \equiv \alpha_1\alpha'_2 \equiv \alpha'_1\alpha_2 \equiv +1, \qquad (\text{mod } 3).$$

Avec ces conventions, 12 couples canoniques associés comprennent 2 couples conjugués unitaires positifs, les 2 couples opposés négatifs et leurs 8 *produits*, par les 2 couples conjugués de décomposition de 1, qui ne sont plus unitaires.

7. Cette composition s'étend de proche en proche à un système de h paires de couples conjugués, canoniques premiers entre eux deux à deux (éventuellement unitaires) elle donne 2^{h-1} paires de produits de chacun h composants. Elle permet d'énoncer une nouvelle propriété caractéristique d'un couple canonique.

Pour qu'un couple d'entiers (de $\mathbf{E}_j$) *soit canonique, il faut et il suffit que leur norme commune soit un produit de facteurs premiers* (rationnels) *différents, chacun étant congru à* $+1$ (mod 3).

$$a = \mathrm{N}(\alpha) = \mathrm{N}(\alpha') = \prod_x p_x; \qquad \begin{cases} x \text{ de } 1 \text{ à } h; & p_x \text{ premier}; \\ \text{les } p_x \text{ inégaux}; & p_x \equiv +1 \ (\text{mod } 3). \end{cases}$$

La condition est nécessaire. — Si a admettait un facteur q, congru à -1, (mod 3), ou le facteur 3, le nombre q premier dans $\mathbf{E}_j$, ou le nombre $(j-j')$, diviserait les deux conjugués α et α' qui ne seraient pas premiers entre eux. Si a admettait un facteur carré p^2, le nombre premier p étant décomposable en $\varpi\varpi'$, le facteur rationnel $\varpi\varpi'$ ou l'un des facteurs carrés ϖ^2 ou ϖ'^2 diviserait α.

La condition est suffisante. — Si un nombre entier rationnel a est décomposé comme il est dit, il peut être obtenu comme norme d'un couple canonique unitaire positif de 2^{h-1} façons. Il suffit de décomposer chaque nombre p_x en un produit de nombres (premiers) d'un couple unitaire positif, ce qui donne 2 couples conjugués (seulement)

$$\|\varpi_x \quad \varpi'_x\|, \qquad \|\varpi'_x \quad \varpi_x\|; \qquad p_x = \varpi_x\varpi'_x, \qquad \varpi_x \equiv \varpi'_x \equiv +1, \qquad (\text{mod } 3)$$

puis de multiplier de proche en proche, ce qui donne 2^{h-1} paires de couples unitaires positifs. Les autres sont obtenues en prenant les opposés d'une part, et en multipliant par les couples non unitaires de norme 1 d'autre part. Ceci donne 2^{h-1} systèmes différents de 12 couples associés.

8. Pour obtenir pratiquement les couples canoniques unitaires, il est commode de calculer les valeurs de la forme

$$a^2 + a'^2 - aa' \qquad \begin{cases} a,\ a' \text{ entiers rationnels, positifs ou négatifs;} \\ a \equiv a' \equiv -1, \quad (\text{mod } 3); \end{cases}$$

il suffit de retenir les valeurs qui sont sans facteur carré. En outre, comme il y a symétrie en a, a', il suffit de limiter les calculs aux couples de nombres tels que

$$|a'| < |a|,$$

chaque couple unitaire n'est ainsi obtenu qu'une fois.

La considération des différences premières et secondes (qui sont constantes pour une même valeur de a ou de a') permet de simplifier le calcul du tableau de valeurs. L'exemple ci-dessous contient tous les couples de norme inférieure à 300 ($\alpha = a'j + aj'$).

$a \backslash a'$	-16	-13	-10	-7	-4	-1	2	5	8	11	14
-19	313	283	271	277	301 7×43	~~343~~	403 13×31	481 13×37	577	691	823
-16		217 7×31	~~196~~	193	~~208~~	241	~~292~~	~~361~~	~~448~~	553	~~676~~
-13			139	127	133 7×19	157	199	259 7×37	337	433	
-10				79	~~76~~	91 7×13	~~124~~	~~175~~	~~244~~		
-7					37	43	67	109			
-4						13	~~28~~				
-1						1					
2						7					
5					61	31	19				
8				~~169~~	~~112~~	73	~~52~~	~~49~~			
11			331	247 13×19	181	133 7×19	103	91 7×13	97		
14		547	~~436~~	~~343~~	~~268~~	211	~~172~~	151	~~148~~	163	
17	817 19×43	679 7×97	559 13×43	457	373	307	259 7×37	229	217 7×31	223	247 13×19

Les nombres barrés sont ceux qui ont un facteur carré; les nombres pour lesquels aucune décomposition n'est indiquée sont premiers. Le tableau, ainsi limité, ne contient encore que des nombres composés de un ou deux facteurs; ces derniers s'y trouvent effectivement deux fois.

II. — Génération d'une équation abélienne de degré 3.

1. Je rappelle d'abord ce qu'est une *équation abélienne* de degré 3 dans le corps $\mathcal{R}$ des nombres rationnels. Elle est obtenue en annulant un polynome

$$f(x) = x^3 - sx^2 + s'x - s'',$$

dont les coefficients sont dans $\mathcal{R}$; qui est *irréductible* (ou indécomposable) dans $\mathcal{R}$ (c'est-à-dire encore, dont aucune des 3 racines θ_1, θ_2, θ_3 n'est dans $\mathcal{R}$); enfin qui *admet un groupe* $\mathbf{G}_\sigma$ *abélien du* 3^e *ordre.*

Ce groupe [1] est nécessairement formé de 3 permutations circulaires

$$\|\theta_1\theta_2\theta_3\|.(\sigma) = \|\theta_2\theta_3\theta_1\|; \qquad \|\theta_1\theta_2\theta_3\|.(\sigma^2) = \|\theta_3\theta_1\theta_2\|; \qquad (\sigma^3) = (1).$$

Par la troisième propriété, il faut alors entendre que la condition nécessaire et suffisante pour qu'une expression rationnelle $\varphi(\theta_1, \theta_2, \theta_3)$ à coefficients dans $\mathcal{R}$, ait une valeur dans $\mathcal{R}$ est qu'elle soit invariante pour les substitutions de $\mathbf{G}_\sigma$

$$[\varphi(\theta_1, \theta_2, \theta_3) \in \mathcal{R}] \rightleftharpoons [\varphi(\theta_1, \theta_2, \theta_3) = \varphi(\theta_2, \theta_3, \theta_1) = \varphi(\theta_3, \theta_1, \theta_2)].$$

Ce polynome $f(x)$, considéré dans le corps $\mathbf{R}_j$, étudié ci-dessus, y reste irréductible, sinon il ne pourrait y avoir plus de deux racines conjuguées et la troisième serait rationnelle. Il conserve le même groupe $\mathbf{G}_\sigma$, sinon il ne pourrait admettre que son seul sous groupe, constitué par la seule transformation identique, et chaque θ_i serait un nombre de $\mathbf{R}_j$.

---

[1] Je représente une *transformation*, ou, plus exactement, son *opérateur* par une lettre entre parenthèses (σ), (s), ... et je la place en multiplicateur à droite, séparée par un point de l'élément (nombre, matrice, ensemble, ...) à transformer. La formule du texte se lit ainsi : (σ) remplace les nombres θ_1, θ_2, θ_3, respectivement par θ_2, θ_3, θ_1.

Le *produit de deux transformations*, désigné par le signe $\times$ est alors défini par la relation

$$X.(\sigma_1 \times \sigma_2) = [(X.(\sigma_1)].(\sigma_2),$$

X désigne un élément quelconque qui peut être transformé par (σ_1) et la formule suppose que le résultat de cette transformation peut, à son tour être transformé par (σ_2). Le produit ainsi défini s'étend, sous les réserves faites, à un nombre quelconque de transformations: il est *associatif*, mais non nécessairement commutatif.

La *transformation identique* est désignée par (1); l'*inverse* de (σ), désignée par (σ^{-1}), est, si elle existe, la transformation telle que

$$(\sigma) \times (\sigma^{-1}) = (\sigma^{-1}) \times (\sigma) = (1),$$

ou

$$[X.(\sigma) = Y] \rightleftharpoons [X = Y.(\sigma^{-1})].$$

Ces notations, dont on pourrait se passer dans l'étude présente, amorcent une généralisation possible.

2. Pour obtenir une autre propriété caractéristique, j'utilise les *résolvantes de* Lagrange des nombres θ_u que je note par la même lettre surlignée et qui sont [u défini (mod 3)]

$$(1) \qquad \bar\theta_u = \theta_u + j\theta_{u+1} + j'\theta_{u+2}, \qquad \bar\theta'_u = \theta_u + j'\theta_{u+1} + j\theta_{u+2}.$$

Je puis encore les écrire

$$\bar\theta_u = \Sigma_v j^v \theta_{u+v}, \qquad \bar\theta'_u = \Sigma_v j'^v \theta_{u+v}, \qquad (u,\ v \text{ définis mod } 3).$$

Le changement de u en $u+1$, ou en $u+2$, est obtenu, soit par une permutation circulaire (σ), ou (σ^2), des θ_u, soit en multipliant la résolvante considérée par j ou j'

$$\bar\theta_{u+1} = \bar\theta_u.(\sigma) = j'\bar\theta_u, \qquad \bar\theta'_{u+1} = \bar\theta'_u.(\sigma) = j\bar\theta'_u,$$
$$\bar\theta_{u+2} = \bar\theta_u.(\sigma^2) = j\bar\theta_u, \qquad \bar\theta'_{u+2} = \bar\theta'_u.(\sigma^2) = j'\bar\theta'_u.$$

Avec ces notations la propriété annoncée peut être exprimée :

La condition nécessaire et suffisante pour que le polynome $f(x)$, de degré 3, à coefficients dans $\mathcal{R}$ et dont les racines sont θ_1, θ_2, θ_3, *soit abélien est que les deux résolvantes de* Lagrange (de même indice u) *des racines, vérifient la relation*

$$(2) \qquad \bar\theta_u^2 = \alpha\bar\theta'_u, \qquad \bar\theta'^2_u = \alpha'\bar\theta_u,$$

où α et α' sont des nombres conjugués de $\mathbf{R}_j$, tels que les nombres

$$(3) \qquad \alpha^2\alpha' = \mathrm{N}(\alpha)\alpha, \qquad \alpha'^2\alpha = \mathrm{N}(\alpha)\alpha'$$

ne soient pas des puissances cubiques exactes dans $\mathbf{R}_j$.

Si les relations (2) sont vérifiées pour une valeur de l'indice u (mod 3), elles le sont pour les deux autres, d'après les propriétés indiquées. D'autre part, il suffit que la restriction (3) soit vérifiée pour l'un des deux nombres, elle l'est alors manifestement pour l'autre qui est son conjugué. Elle implique notamment que α ne soit pas un nombre rationnel a qui serait égal à son conjugué α', ce qui entraînerait $\alpha^2\alpha' = a^2 a = a^3$.

3. Avant de démontrer la propriété, j'indique quelques transformations et conséquences des conditions annoncées.

Les relations (2) sont équivalentes au système surabondant

$$(2') \qquad \begin{cases} \bar\theta_u^3 = \alpha^2\alpha', \\ \bar\theta'^3_u = \alpha'^2\alpha, \end{cases} \qquad \bar\theta_u\bar\theta'_u = \alpha\alpha'.$$

Si ces nouvelles relations sont vérifiées pour une valeur de l'indice u, elles le sont encore pour les deux autres. Cette invariance pour l'indice et la symétrie des relations en $\bar\theta_u$, $\bar\theta'_u$ et α, α' peuvent être exprimées par des transformations.

Le système (2′), ou le système (2), est invariant pour les transformations du groupe (abélien) $\mathbf{G}_{\sigma,\varepsilon}$, dont la loi de composition est exprimée par

$$(\sigma),\quad (\sigma^2),\quad (\sigma^3)=(\varepsilon^2)=(1),\qquad (\sigma\varepsilon)=(\varepsilon\sigma),$$

et dont les transformations génératrices (σ), (ε) sont définies par

$$\|\bar\theta_u\bar\theta'_u j\|.(\sigma)=\|\bar\theta_{u+1}\bar\theta'_{u+1}j\|,\qquad \|\bar\theta_u\bar\theta'_u j\|.(\varepsilon)=\|\bar\theta'_u\bar\theta_u j'\|;$$

où l'indice v est défini (mod 3). Il en résulte les effets des autres transformations du groupe

$$\|\bar\theta_u\bar\theta'_u j\|.(\sigma^2)=\|\bar\theta_{u+2}\bar\theta'_{u+2}j\|,$$
$$\|\bar\theta_u\bar\theta'_u j\|.(\sigma\varepsilon)=\|\bar\theta_u\bar\theta'_u j\|.(\varepsilon\sigma)=\|\bar\theta'_{u+1}\bar\theta_{u+1}j'\|,$$
$$\|\bar\theta_u\bar\theta'_u j\|.(\sigma^2\varepsilon)=\|\bar\theta_u\bar\theta'_u j\|.(\varepsilon\sigma^2)=\|\bar\theta'_{u+2}\bar\theta_{u+2}j'\|.$$

D'autre part les équations (1) de même indice, complétées par la valeur (rationnelle) de la somme des racines (*trace* de chacune d'elles)

$$\theta_u+\theta_{u+1}+\theta_{u+2}=s,$$

déterminent en fonction de $\bar\theta_u$, $\bar\theta'_u$, j, j' et s ces racines dont les expressions sont

$$(1')\qquad \theta_u=\frac{1}{3}(\bar\theta_u+\bar\theta'_u+s);\qquad \text{ou}\qquad (3\theta_u-s)=\bar\theta_u+\frac{\alpha\alpha'}{\bar\theta_u}=\bar\theta'_u+\frac{\alpha\alpha'}{\bar\theta'_u}.$$

Les transformations (σ), (σ^2), $(\sigma^3)=(1)$, permutent circulairement ces racines et $(\sigma\varepsilon)$, $(\sigma^2\varepsilon)$, (ε) donnent respectivement les mêmes résultats

$$\theta_u.(\sigma)=\theta_u.(\sigma\varepsilon)=\theta_{u+1};\qquad \theta_u.(\sigma^2)=\theta_u.(\sigma^2\varepsilon)=\theta_{u+2};\qquad \theta_u.(\varepsilon)=\theta_u.$$

Le groupe $\mathbf{G}_\sigma$ est par suite égal, ou, plus exactement isomorphe au *groupe quotient* $|\mathbf{G}_{\sigma,\varepsilon}|[1,(\varepsilon)]$.

4. Les expressions (1′) des racines θ_u permettent de calculer leurs fonctions symétriques élémentaires, c'est-à-dire les coefficients s' et s'' du polynome $f(\boldsymbol{x})$ qui les admet pour zéros. Je puis aussi éliminer $\bar\theta_u$ et $\bar\theta'_u$ entre (1′) et (2′). L'équation (1′) entraîne

$$\left(\theta_u-\frac{s}{3}\right)^3=\frac{1}{27}(\bar\theta_u+\bar\theta'_u)^3=\frac{1}{27}(\bar\theta_u^3+\bar\theta_u'^3)+\frac{1}{9}\bar\theta_u\bar\theta'_u(\bar\theta_u+\bar\theta'_u);$$

les conditions (2′) permettent d'en éliminer $\bar\theta_u$, $\bar\theta'_u$; ce qui donne

$$(4)\qquad \left(\theta_u-\frac{s}{3}\right)^3-\frac{\alpha\alpha'}{3}\left(\theta_u-\frac{s}{3}\right)-\frac{1}{27}(\alpha\alpha'\alpha+\alpha')=0,$$

ou, sous forme développée,

$$(4')\qquad \theta_u^3-s\,\theta_u^2+\frac{1}{3}(s^2-\alpha\alpha')\,\theta_u-\frac{1}{27}[s^3-3s\alpha\alpha'+\alpha\alpha'(\alpha+\alpha')]=0.$$

Le *discriminant* de cette équation est

$$-\prod_{u,v}(\theta_u-\theta_v)=-\frac{1}{27}(\alpha\alpha')^2(\alpha-\alpha')^2; \qquad (u\neq v, \quad u, v=1, 2, 3).$$

Je signale encore que les résolvantes $\bar{\theta}_u$ et $\bar{\theta}'_u$ peuvent être exprimées par des fonctions rationnelles de *l'une* des racines θ_u, à coefficients dans $\mathbf{R}_j$. Il suffit de rapprocher les équations en $\bar{\theta}_u$ ou $\bar{\theta}'_u$ des systèmes (2′) et (1′)

$$\begin{cases} \bar{\theta}_u^3-\alpha^2\alpha'=0, \\ \bar{\theta}_u+\dfrac{\alpha\alpha'}{\bar{\theta}_u}-3\left(\theta_u-\dfrac{s}{3}\right)=0 \end{cases} \qquad \begin{cases} \bar{\theta}'^3_u-\alpha'^2\alpha=0, \\ \bar{\theta}'_u+\dfrac{\alpha\alpha'}{\bar{\theta}'_u}-3\left(\theta_u-\dfrac{s}{3}\right)=0 \end{cases}$$

et chercher le p. g. c. d. linéaire en $\bar{\theta}_u$ et $\bar{\theta}'_u$ des premiers membres

$$(1'') \qquad \bar{\theta}_u=\frac{\alpha\alpha'[(3\theta_u-s)+\alpha]}{(3\theta_u-s)^2-\alpha\alpha'}, \qquad \bar{\theta}'_u=\frac{\alpha\alpha'[(3\theta_u-s)+\alpha']}{(3\theta_u-s)^2-\alpha\alpha'}.$$

5. *La condition est nécessaire.* — Je suppose l'équation abélienne; les quotients

$$\bar{\theta}_u^2:\bar{\theta}'_u=\frac{(\theta_u+j\theta_{u+1}+j'\theta_{u+2})^2}{(\theta_u+j'\theta_{u+1}+j\theta_{u+2})}, \qquad \bar{\theta}'^2_u:\bar{\theta}_u=\frac{(\theta_u+j'\theta_{u+1}+j\theta_{u+2})^2}{(\theta_u+j\theta_{u+1}+j'\theta_{u+2})}$$

sont laissés invariants par les permutations circulaires de $\mathbf{G}_\sigma$; par suite leurs valeurs appartiennent à $\mathbf{R}_j$. En outre je puis passer de l'une à l'autre en transposant j et j', ces valeurs sont donc des nombres conjugués α, α' de $\mathbf{R}_j$; ce qui démontre les relations (2).

Le nombre $\alpha^2\alpha'$ ne peut être une puissance cubique exacte, sinon les $\bar{\theta}_u$, d'après les relations (2′), seraient dans $\mathbf{R}_j$; il en serait de même des θ_u, d'après les relations (1′), et le polynome $f(x)$ ne serait pas irréductible (dans $\mathbf{R}_j$, ni par suite dans $\mathcal{R}$).

6. *La condition est suffisante.* — Je suppose vérifiées les conditions (1) et (2) et les nombres conjugués α, α' exprimés par leurs formes canoniques (conjuguées) :

$$\alpha=aj+a'j'; \qquad \alpha'=aj'+a'j; \qquad (a, a' \text{ dans } \mathcal{R}).$$

Leur norme que je désigne par m et leur trace sont des nombres de $\mathcal{R}$

$$m=\alpha\alpha'=a^2+a'^2-aa', \qquad \alpha+\alpha'=-(a+a').$$

Le polynome $f(x)$, qui a pour racines les θ_u, est, avec ces notations,

$$f(x)=\left(x-\frac{s}{3}\right)^3-\frac{m}{3}\left(x-\frac{s}{3}\right)+\frac{m}{27}(a+a')$$

et son discriminant est

$$\frac{m^2}{9}(a-a')^2.$$

Ce polynome est irréductible, sinon l'une des racines θ_u serait dans $\mathcal{R}$; la résolvante $\bar{\theta}_u$, donnée par la relation (1″) serait dans $\mathbf{R}_j$ et $\alpha^2\alpha'$ serait une puissance cubique exacte (dans $\mathbf{R}_j$).

D'autre part les équations (2′) montrent que j et j' peuvent être exprimés sous forme d'expressions rationnelles, à coefficients dans $\mathcal{R}$, d'un quelconque des $\bar{\theta}_u$ (ou des $\bar{\theta}'_u$)

$$j = \frac{\bar{\theta}_u^3 + ma'}{m(a-a')};\qquad j' = \frac{\bar{\theta}_u^3 + ma}{m(a'-a)}.$$

Il en est par suite de même de tous les $\bar{\theta}_u$ et $\bar{\theta}'_u$, puis des θ_u, par application des relations (1′). Je puis exprimer ces deux propriétés en disant que chacun des $\bar{\theta}_u$ est un *élément primitif* du corps $\mathbf{R}_{\theta,j}$ engendré par les θ_u et j, j'; les conjugués de cet élément sont les 6 valeurs $\bar{\theta}_u$ et $\bar{\theta}'_u$. Les transformations qui font passer de l'élément considéré à chacune d'elles sont celles du groupe $\mathbf{G}_{\sigma,\varepsilon}$. Relativement aux θ_u, elles se répartissent dans les trois classes du *groupe quotient*

$$\mathbf{G}_{\sigma,\varepsilon} \mid (1, \varepsilon),$$

qui est isomorphe à $\mathbf{G}_\sigma$ et j'ai ainsi obtenu le groupe de l'équation qui est bien abélienne.

7. J'aurais pu aussi remarquer que la racine carrée du discriminant

$$(\theta_1-\theta_2)(\theta_2-\theta_3)(\theta_3-\theta_1) = \pm\frac{m(a-a')}{3}$$

est un nombre rationnel et que les trois permutations circulaires de $\mathbf{G}_\sigma$ qui la laissent invariante forment le groupe de l'équation.

Le polynome étant abélien, ses trois racines peuvent être exprimées dans $\mathcal{R}$, en fonctions rationnelles de l'une d'elles. Je puis obtenir ces expressions en utilisant les relations (1′) pour calculer les carrés et les produits deux à deux des θ_u, les relations (2) et (2′) permettent de les exprimer en fonctions linéaires des $\bar{\theta}_u$, $\bar{\theta}'_u$; et les relations (1) les donnent en fonction des θ_u (dans $\mathbf{R}_j$)

$$\begin{aligned} 9\theta_u^2 &= \theta_u(\alpha+\alpha'+4s) + \theta_{u+1}(j'\alpha+j\,\alpha'-2s) + \theta_{u+2}(j\,\alpha+j'\alpha'-2s) + 2\alpha\alpha'+s^2,\\ 9\theta_{u+1}\theta_{u+2} &= \theta_u(\alpha+\alpha'-2s) + \theta_{u+1}(j\,\alpha+j'\alpha'+\ s) + \theta_{u+2}(j'\alpha+j\,\alpha'+\ s) - \ \alpha\alpha'+s^2.\end{aligned}$$

Les parenthèses sont des nombres de $\mathcal{R}$ et ces formules constituent une table de multiplication dans le corps $\mathbf{R}_\theta$. La première donne l'expression de θ_{u+1} ou θ_{u+2}, sous forme d'un polynome du 2e degré en θ_u (en éliminant θ_{u+2} ou θ_{u+1}, au moyen de la trace s).

Le raisonnement fait pour montrer que la valeur de $\bar{\theta}_u^2 : \bar{\theta}'_u$ est dans $\mathbf{R}_j$ est valable pour un monome convenable des deux résolvantes.

La valeur de

$$\bar{\theta}_u^a\bar{\theta}'^{a'}_u;\qquad a-a'\equiv 0,\qquad (\text{mod } 3);$$

est un nombre de $\mathbf{R}_j$.

En effet une permutation circulaire (σ) multiplie ce monome par

$$j'^{a} j^{a'} = j^{a'-a} = 1,$$

donc le laisse invariable. Sa valeur peut d'ailleurs s'exprimer au moyen de α, α'

$$\bar{\theta}_u^a \bar{\theta}'^{a'}_u = \alpha^{\frac{2a+a'}{3}} \alpha'^{\frac{a+2a'}{3}}.$$

Les valeurs ainsi obtenues (dans $\mathbf{R}_j$), constituent un groupe abélien de générateurs α, α'

$$\alpha^x \alpha'^{x'}; \qquad (x,\ x' \text{ entiers quelconques};\ a = 2x - x';\ a' = 2x' - x).$$

Les expressions de ces monomes comprennent, comme cas particuliers, les formules (2) et (2'); elles amorcent la généralisation du raisonnement pour les corps abéliens de degré quelconque.

8. La propriété ainsi démontrée peut être remplacée et complétée par la suivante :

Il y a correspondance biunivoque entre un système

$$\| \alpha \quad \alpha' \| \quad \text{et} \quad s; \qquad [\alpha, \alpha' \in \mathrm{R}_j;\ s \in \mathcal{R}]$$

[formé d'un couple de $\mathbf{R}_j$, vérifiant la condition (3) et d'une trace s], *et un triplet* $\| \theta_1 \quad \theta_2 \quad \theta_3 \|$ *de racines d'une équation abélienne, ordonné à une permutation circulaire près.*

Les démonstrations précédentes indiquent comment le couple et la trace sont définis à partir du triplet, et, inversement comment le triplet peut être construit à partir de la trace et du couple. Je rassemble les formules essentielles de cette construction

$$(2' \text{ et } 1') \qquad \begin{matrix} \bar{\theta}_1^3 = \alpha^2 \alpha', \\ \bar{\theta}_1 \bar{\theta}'_1 = \alpha\alpha', \end{matrix} \qquad \left\{ \begin{aligned} \theta_1 &= \frac{1}{3}(\bar{\theta}_1 + \bar{\theta}'_1 + s), \\ \theta_2 &= \frac{1}{3}(j'\bar{\theta}_1 + j\,\bar{\theta}'_1 + s), \\ \theta_3 &= \frac{1}{3}(j\,\bar{\theta}_1 + j'\bar{\theta}'_1 + s). \end{aligned} \right.$$

L'équation en $\bar{\theta}_1$ en donne trois valeurs possibles, produits de l'une d'elles par 1, j ou j'; le remplacement de l'une de ces valeurs par une autre permute circulairement les nombres du triplet, ce qui démontre complètement l'énoncé.

Le remplacement du couple par son conjugué

$$\| \alpha' \quad \alpha \| \quad \text{substitué à} \quad \| \alpha \quad \alpha' \|,$$

transpose $\bar{\theta}_1$ et $\bar{\theta}'_1$, et par suite *transpose deux nombres du triplet*

$$\| \theta_1 \quad \theta_3 \quad \theta_2 \| \quad \text{substitué à} \quad \| \theta_1 \quad \theta_2 \quad \theta_3 \|.$$

Le remplacement simultané du couple et de la trace par leurs opposés

$$(\ \| -\alpha \quad -\alpha' \|\ \text{et}\ -s) \qquad \text{substitués à} \qquad (\ \| \alpha \quad \alpha' \|\ \text{et}\ s);$$

remplace le triplet par son opposé

$$\| -\theta_1 \quad -\theta_2 \quad -\theta_3 \| \qquad \text{substitué à} \qquad \| \theta_1 \quad \theta_2 \quad \theta_3 \|.$$

Le remplacement du couple par un associé (produit par $\| j \quad j' \|$ ou $\| j' \quad j \|$) sera étudié ci-dessous comme cas particulier du produit de deux couples.

9. La construction qui donne les θ_u peut encore être faite si la construction restrictive (3) n'est pas remplie, c'est-à-dire si

$$\alpha^2\alpha' = \delta^3 = (dj + d'j')^3; \qquad \alpha'^2\alpha = \delta'^3 = (dj' + d'j)^3; \qquad [d,\ d' \in \mathcal{R}].$$

Le polynome $f(x)$ a ses racines dans $\mathcal{R}$ et leurs expressions sont déduites immédiatement des équations (2′) et (1′)

$$\theta_1 = \delta, \qquad \theta_2 = j\delta, \qquad \theta_3 = j'\delta; \qquad \theta'_1 = \delta', \qquad \theta'_2 = j'\delta', \qquad \theta'_3 = j\delta';$$

et

$$(1\text{-}d) \qquad \begin{cases} \theta_1 = \dfrac{1}{3}\ (\delta + \delta' + s) = \dfrac{1}{3}(s - d - d'), \\ \theta_2 = \dfrac{1}{3}\ (j\delta + j'\delta' + s) = \dfrac{1}{3}(s - d + 2d'), \\ \theta_3 = \dfrac{1}{3}(j'\delta + j\delta' + s) = \dfrac{1}{3}(s + 2d - d'). \end{cases}$$

La valeur de α peut d'ailleurs être exprimée dans ce cas au moyen de d et d'

$$\alpha = \frac{\delta^2}{\delta'} = \frac{\delta^3}{\mathrm{N}(\delta)} = \frac{(3\,dd'^2 - d^3 - d'^3)j' + (3\,d^2d' - d^3 - d'^3)j}{d^2 + d'^2 - dd'}.$$

Les racines ainsi obtenues vérifient les mêmes relations à coefficients rationnels que les racines des équations irréductibles, et notamment les formules de multiplication du numéro précédent. Si $\alpha = 0$, les θ_i sont des nombres rationnels égaux entre eux $\left(\text{et à } \dfrac{s}{3}\right)$.

10. De ce qui précède, je puis déduire la condition pour qu'un polynome du 3ᵉ degré, à coefficients rationnels soit abélien. Je puis toujours l'écrire sous la forme

$$f(x) = \left(x - \frac{s}{3}\right)^3 + p\left(x - \frac{s}{3}\right) + q;$$

il faut et il suffit qu'il soit irréductible et qu'il existe un couple α, α' de nombres conjugués dans $\mathbf{R}_j$ tels que (équation 4)

$$\frac{\alpha\alpha'}{3} = -p, \qquad -\frac{1}{27}\alpha\alpha'(\alpha + \alpha') = q.$$

Les nombres α, α' sont ainsi déterminés par une équation du 2e degré

$$x^2 - \frac{9q}{p}x - 3p = 0,$$

dont il est nécessaire et suffisant que le discriminant soit le produit de -3 par un carré (de nombre rationnel). Il en résulte l'énoncé :

Pour que le polynome

$$f(x) = \left(x - \frac{s}{3}\right)^3 + p\left(x - \frac{s}{3}\right) + q, \qquad (s, p, q \text{ rationnels}),$$

soit abélien, il faut et il suffit qu'il soit irréductible et que le nombre $-(4p^3 + 27q^2)$ *soit le carré d'un nombre rationnel.*

Si la condition du carré était seule remplie, le polynome n'étant plus irréductible aurait des racines rationnelles données par les formules (1-d); ce sont d'ailleurs des nombres rationnels quelconques.

11. On pourrait appliquer un raisonnement analogue au précédent pour construire une *équation du second degré* dans $\mathcal{R}$ (nécessairement abélienne, si elle est irréductible). Ses deux racines conjuguées étant θ_1 et θ_2, la « *résolvante* de Lagrange » (construite avec -1, racine carrée de 1) est

$$\bar{\theta}_1 = \theta_1 + (-1)\theta_2 = \theta_1 - \theta_2.$$

Son carré doit être un nombre rationnel d, non carré parfait. Le polynome cherché est, en appelant s la trace,

$$f(x) = \left(x - \frac{s}{2}\right)^2 - d = x^2 - sx + \frac{1}{4}(s^2 - 4d).$$

Il y a correspondance univoque entre un système

$$d \text{ et } s; \qquad (d \text{ et } s \in \mathcal{R});$$

(formé d'un nombre de $\mathcal{R}$, non carré et d'une trace s), *et un couple* $\|\theta_1 \quad \theta_2\|$, *de racines d'une équation du second degré, ordonné à une transposition près* (ou encore non ordonné).

III. — Génération d'un corps abélien.

1. Je vais étudier le *corps abélien* $\mathbf{R}_0$, constitué par toutes les fonctions $\vartheta = \varphi(\theta)$, rationnelles, à coefficients rationnels de l'un des nombres θ d'un triplet $\|\theta_1 \quad \theta_2 \quad \theta_3\|$ de racines d'une équation abélienne de degré 3. Ce corps contient les *conjugués* $\vartheta_u = \varphi(\theta_u)$ de chacun de ses éléments (et notamment ceux de θ). En outre l'ordre d'un triplet de conjugués $\|\vartheta_u \quad \vartheta_{u+1} \quad \vartheta_{u+2}\|$ est déterminé, à une permutation circulaire près, lorsque l'ordre des θ_u est choisi.

Deux conjugués quelconques de θ forment avec 1 une *base du corps* (ou sont *arithmétiquement indépendants*). En effet s'il existait entre eux une relation linéaire, à coefficients rationnels

$$a+b\theta_{u+1}+c\theta_{u+2}=0; \qquad (a,\ b,\ c \text{ rationnels});$$

elle subsisterait par permutation circulaire des θ_u; or ceci n'est pas possible, car les trois relations linéaires en a, b, c ainsi obtenues ont un déterminant non nul

$$\begin{vmatrix} 1 & 1 & 1 \\ \theta_1 & \theta_2 & \theta_3 \\ \theta_2 & \theta_3 & \theta_1 \end{vmatrix} = -(\theta_1+j\theta_2+j'\theta_3)(\theta_1+j'\theta_2+j\theta_3) = -\alpha\alpha' \neq 0.$$

Tout élément $\mathfrak{I}$ de $\mathbf{R}_0$ peut donc être exprimé d'une et d'une seule façon, par une fonction linéaire à coefficients rationnels de 1 et de 2 conjugués de θ. Le triplet de ses conjugués, ordonné, à une permutation circulaire près, est défini par une égalité de matrices

$$\| \mathfrak{I}_u \quad \mathfrak{I}_{u+1} \quad \mathfrak{I}_{u+2} \| = \| a \quad b \quad c \| \times \begin{Vmatrix} 1 & 1 & 1 \\ \theta_{u+1} & \theta_{u+2} & \theta_u \\ \theta_{u+2} & \theta_u & \theta_{u+1} \end{Vmatrix}; \qquad (a,\ b,\ c \text{ rationnels}).$$

2. Ces propriétés permettent de remplacer l'appartenance de deux triplets à un même corps, par une relation entre les couples correspondants de $\mathbf{R}_j$.

La condition nécessaire et suffisante pour qu'aux systèmes

$$\| \alpha \quad \alpha' \| \text{ et } s; \qquad \| \beta \quad \beta' \| \text{ et } s';$$

(couple et trace), *correspondent des triplets de racines*

$$\| \theta_1 \quad \theta_2 \quad \theta_3 \|, \qquad \| \mathfrak{I}_1 \quad \mathfrak{I}_2 \quad \mathfrak{I}_3 \|$$

appartenant à un même corps abélien et ordonnés de même façon, à une permutation circulaire près, *est que l'un des quotients*

$$(\alpha^2\alpha' : \beta^2\beta') \qquad \text{ou} \qquad (\alpha'^2\alpha : \beta'^2\beta)$$

soit, dans R_j, *une puissance cubique exacte.*

Si la condition est remplie pour l'un des quotients, elle l'est évidemment pour l'autre qui est le nombre conjugué.

3. *La condition est nécessaire.* — Je suppose le triplet des $\mathfrak{I}_u$ dans le corps des θ_u et ordonné comme eux; je calcule ses résolvantes de Lagrange par une égalité de matrices

$$\| \bar{\mathfrak{I}}_1 \quad \bar{\mathfrak{I}}'_1 \| = \| \mathfrak{I}_1 \quad \mathfrak{I}_2 \quad \mathfrak{I}_3 \| \times \begin{Vmatrix} 1 & 1 \\ j & j' \\ j' & j \end{Vmatrix} = \| a \quad b \quad c \| \times \begin{Vmatrix} 1 & 1 & 1 \\ \theta_2 & \theta_3 & \theta_1 \\ \theta_3 & \theta_1 & \theta_2 \end{Vmatrix} \times \begin{Vmatrix} 1 & 1 \\ j & j' \\ j' & j \end{Vmatrix}$$

$$= \| b\bar{\theta}_2 + c\bar{\theta}_3 \quad b\bar{\theta}'_2 + c\bar{\theta}'_3 \| = \| \bar{\theta}_1(bj'+cj) \quad \bar{\theta}'_1(bj+cj') \|.$$

J'en conclus la condition nécessaire entre les nombres du couple

$$\beta^2\beta' = \bar\vartheta_1^3 = \bar\theta_1^3(bj'+cj)^3 = \alpha^2\alpha'(bj'+cj)^3.$$

La condition est suffisante. — Je suppose la condition vérifiée, j'en déduis la relation entre les résolvantes de Lagrange des triplets correspondants

$$\bar\vartheta_1^3 : \bar\theta_1^3 = [(\beta^2\beta'):(\alpha^2\alpha')] = (bj'+cj)^3, \qquad \bar\vartheta_1'^3 : \bar\theta_1'^3 = (bj+cj')^3;$$

je puis choisir les indices de façon que

$$\begin{aligned}
&\bar\vartheta_1 = \bar\theta_1(bj'+cj), &&\bar\vartheta_2 = \bar\vartheta_1 j' = \bar\theta_2(bj'+cj), &&\bar\vartheta_3 = \bar\vartheta_1 j = \bar\theta_3(bj'+cj),\\
&\bar\vartheta'_1 = \bar\theta'_1(bj+cj'), &&\bar\vartheta'_2 = \bar\vartheta'_1 j = \bar\theta'_2(bj+cj'), &&\bar\vartheta'_3 = \bar\vartheta'_1 j' = \bar\theta'_3(bj+cj').
\end{aligned}$$

Je calcule alors ϑ_u, en me donnant sa trace s' et en appliquant (1')

$$\begin{aligned}
3\vartheta_u = (\bar\vartheta_u + \bar\vartheta'_u + s') &= b(\bar\theta_u j' + \bar\theta'_u j) + c(\bar\theta_u j + \bar\theta'_u j') + s'\\
&= b(\theta_{u+1} + \theta'_{u+1}) + c(\theta_{u+2} + \theta'_{u+2}) + s'\\
&= 3b\theta_{u+1} + 3c\theta_{u+2} + s' - s(b+c).
\end{aligned}$$

Ceci entraîne l'égalité des matrices indiquée ci-dessus, ce qui montre que le triplet des ϑ_u est dans le corps défini et ordonné par le triplet des θ_u.

La condition ne fait pas intervenir les traces s, s' de sorte que deux triplets correspondant à un même couple et de traces différentes sont dans un même corps. Ceci était évident *a priori*, car le changement de trace augmente seulement chaque nombre du triplet d'un même nombre rationnel.

4. Je puis ainsi choisir, dans un corps abélien, un *triplet canonique*, correspondant à un couple particulièrement simple de $\mathbf{R}_j$, c'est ce que je précise par l'énoncé suivant.

Parmi les couples de $\mathbf{R}_j$ *auxquels correspondent les triplets ordonnés d'un même corps abélien*, de degré 3, *il en existe deux, opposés, et deux seulement, qui sont canoniques* (§ I, n^{os} 4 et 7). Je les appelle *couples générateurs du corps*.

J'utilise la deuxième propriété caractéristique indiquée pour un facteur canonique : α et α' entiers; l'un d'eux et par suite l'autre sans facteur rationnel, sans facteur commun avec 3 et sans facteur carré.

Je considère un couple quelconque $\|\beta \quad \beta'\|$, engendrant un triplet ordonné de $\mathbf{R}_\theta$; dans les expressions canoniques de ses nombres en j et j', je mets en facteur le p. g. c. d. des coefficients;

$$\beta = \frac{m}{d}(aj+a'j') = \frac{m}{d}\alpha, \qquad \beta' = \frac{m}{d}(aj'+a'j) = \frac{m}{d}\alpha',$$

(a, a' entiers rationnels, premiers entre eux). Pour définir le corps je puis remplacer le couple $\|\beta \quad \beta'\|$ par le couple $\|\alpha \quad \alpha'\|$, car

$$(\alpha^2\alpha'):(\beta^2\beta') = \frac{d^3}{m^3},$$

le nouveau couple est formé de nombres entiers, sans facteur rationnel.

Si l'entier α a un facteur carré, il en est de même de son conjugué :

$$\alpha = \alpha_1\gamma^2, \qquad \alpha' = \alpha'_1\gamma'^2.$$

Je puis alors remplacer

$$|\,\alpha \quad \alpha'\,| \quad \text{par} \quad |\,\alpha_1\gamma' \quad \alpha'_1\gamma\,|,$$

car

$$(\alpha_1\gamma')^2(\alpha'_1\gamma):\alpha^2\alpha' = (1:\gamma)^3.$$

En effectuant ce remplacement plusieurs fois s'il y a lieu (notamment si γ contenait lui-même un facteur carré), je puis obtenir un couple dont les nombres n'ont plus de facteur carré.

Si l'entier α est divisible par $(j-j')$, facteur de 3 (et non par son carré qui est rationnel), il en est de même de son conjugué

$$\alpha = (j-j')\alpha_0, \qquad \alpha' = (j'-j)\alpha'_0.$$

Je puis alors prendre pour nouveau couple $\|\alpha_0 \quad \alpha'_0\|$ car

$$(\alpha_0^2\alpha'_0):(\alpha^2\alpha') = [1:(j'-j)]^3;$$

et les nombres du nouveau couple sont premiers avec 3.

5. Je puis montrer qu'*il n'y a que deux couples générateurs opposés*, en cherchant la condition pour que deux couples canoniques $\|\alpha_1 \quad \alpha'_1\|$ et $\|\alpha_2 \quad \alpha'_2\|$ engendrent le même corps, ou plus exactement des triplets ordonnés d'un même corps. Le quotient

$$(\alpha_1^2\alpha'_1):(\alpha_2^2\alpha'_2),$$

doit être, dans $\mathbf{R}_j$, une puissance cubique. Je le décompose en un produit de puissances positives et négatives de facteurs premiers. Il faut que chaque facteur figure avec un exposant multiple de 3. Un facteur premier qui divise α_1 ne divise pas α'_1; il doit diviser α_2; sinon il figurerait dans le quotient, ou bien avec l'exposant 2 s'il ne divise aucun des nombres α_2, α'_2, ou bien avec l'exposant 1 s'il divise α'_2. Le raisonnement corrélatif montre que tout facteur premier de α_2 divise α_1. Il s'ensuit que le quotient de ces deux nombres est un diviseur de 1

$$\alpha_2 = \alpha_1\varepsilon, \qquad \alpha'_2 = \alpha'_1\varepsilon; \qquad (\varepsilon = \pm 1, \text{ ou } \pm j, \text{ ou } \pm j').$$

Le quotient a pour valeur

$$(\alpha_1^2\alpha'_1):(\alpha_2^2\alpha'_2) = \varepsilon'^2\varepsilon = \varepsilon',$$

ce n'est une puissance cubique que si $\varepsilon' = \pm 1$; les deux couples sont bien égaux ou opposés.

6. Inversement *un couple canonique* $\|\alpha \quad \alpha'\|$ (α, α' entiers premiers entre eux, sans facteur carré) *est couple générateur d'un corps abélien*, de degré 3, dans lequel il définit un ordre des nombres conjugués des triplets.

Si α est de norme différente de 1, j'utilise la décomposition en facteurs premiers

$$\alpha^2\alpha' = \prod_x \varpi_x^2 \varpi_x'; \qquad (x \text{ de } 1 \text{ à } h);$$

les $2h$ facteurs premiers ϖ_x, ϖ_x' sont différents, aucun ne figure au cube dans la décomposition du nombre qui n'est donc pas une puissance cubique exacte; le couple engendre donc une équation irréductible et un corps.

Le couple $\|\alpha' \quad \alpha\|$ engendre le même corps, mais avec un ordre différent dans les triplets (déduit par transposition du précédent).

Les couples $\|j \quad j'\|$ ou $\|j' \quad j\|$ [de décomposition de (1)] engendrent aussi un même corps avec des ordres différents des triplets, car le produit $j^2j' = j$ n'est pas non plus une puissance cubique. Ce corps que je désigne par $\mathbf{R}_{0_0}$, est d'ailleurs défini par les racines de l'équation (obtenue avec une trace nulle)

$$x^3 - \frac{1}{3}x + \frac{1}{27} = 0.$$

7. Un raisonnement analogue peut aussi être fait pour la détermination d'un corps du second degré dont les éléments sont construits comme il a été dit ci-dessus (§ II, n° 10). *La condition nécessaire et suffisante pour qu'à deux systèmes*

$$d \text{ et } s, \qquad d' \text{ et } s'$$

(de carrés des différences et des traces) *correspondent des nombres d'un même corps est que le quotient* ($d:d'$) *soit le carré d'un nombre rationnel.*

Parmi les nombres rationnels, auxquels correspondent des couples de nombres conjugués d'un même corps, du second degré, *il y a un et un seul nombre entier* d (positif ou négatif), *sans facteur carré*. Les couples de nombres du corps sont exprimés par

$$| a + b\sqrt{d} \quad a - b\sqrt{d} |; \qquad (a, b \text{ nombres rationnels}).$$

IV. — Entiers d'un corps abélien.

1. Je rappelle qu'un *entier algébrique* η est une racine d'un polynome $f(x)$, dont les coefficients sont entiers rationnels et dont le terme de plus haut degré a pour coefficient 1. Il suffit que cette condition soit vérifiée pour un polynome quelconque s'annulant pour η, elle est alors également vraie pour le polynome fondamental (irréductible, à coefficients premiers entre eux) du nombre η.

Il en résulte que : les nombres conjugués d'un entier algébrique sont des entiers algébriques; les fonctions symétriques entières à coefficients entiers de ces conjugués sont des entiers rationnels; si un entier algébrique est rationnel, c'est un entier rationnel.

L'ensemble des entiers d'un corps algébrique de degré n est un *anneau* dont les éléments η se déduisent par addition et soustraction de n d'entre eux dont le système est appelé une *base des entiers* (définie à une substitution unimodulaire près)

$$\eta = a_1\eta_1 + a_2\eta_2 + \ldots + a_n\eta_n \qquad (a_i \text{ entiers rationnels}).$$

Le carré du déterminant de la matrice dont les colonnes sont les n conjugués de la base est le *discriminant du corps*. C'est un entier rationnel, indépendant de la base adoptée [dont on démontre qu'il est toujours différent de ± 1].

Je vais étudier la constitution de l'anneau des entiers algébriques d'un corps abélien de degré 3, en distinguant deux cas, suivant que le couple générateur est ou n'est pas *unitaire*; *je donne ce même qualificatif au corps engendré.*

2. Dans un *corps unitaire*, il y a des *bases normales*, c'est-à-dire formées par les trois conjugués d'un entier convenable; l'une d'elles est obtenue en construisant le triplet correspondant au couple générateur (avec une trace convenable). Je précise ces indications par l'énoncé d'une propriété.

Si un corps abélien est unitaire, le triplet de nombres conjugués $\|\theta_1 \quad \theta_2 \quad \theta_3\|$, *construit avec le couple générateur canonique et avec une trace égale à* $+1$ *ou* -1, *suivant que le couple est positif ou négatif, est une base normale des entiers du corps.*

Pour cette raison, je dis que le couple dans $\mathbf{R}_j$ et le triplet dans $\mathbf{R}_0$, définis au signe près, sont *discriminants*; le (nombre) discriminant est d'ailleurs

$$\begin{vmatrix} \theta_1 & \theta_2 & \theta_3 \\ \theta_2 & \theta_3 & \theta_1 \\ \theta_3 & \theta_1 & \theta_2 \end{vmatrix}^2 = [(\theta_1+\theta_2+\theta_3)(\theta_1+j\theta_2+j'\theta_3)(\theta_1+j'\theta_2+j\theta_3)]^2.$$
$$= (1\times\bar\theta_1\times\bar\theta'_2)^2 = (\alpha\alpha')^2.$$

C'est le *carré de la norme D du couple discriminant*. Cette norme D est le produit de h nombres premiers différents, congrus à $+1$ (mod 3), et inversement le carré d'un tel produit D est le discriminant de 2^{h-1} corps unitaires, engendrés par les divers couples unitaires dont D est la norme (§ I, n° 7).

3. Je construis un triplet avec un couple unitaire positif et une trace égale à $+1$ (le changement de signe donnerait un triplet opposé); son polynome fondamental est (formule 4′, § II, n° 4)

$$f(x) = x^3 - x^2 - \frac{1}{3}(1-\alpha\alpha')x - \frac{1}{27}[1 - 3\alpha\alpha' + \alpha\alpha'(\alpha+\alpha')].$$

Je calcule les coefficients en exprimant que le couple est unitaire et positif

$$\alpha = 1 + 3\delta, \qquad \alpha' = 1 + 3\delta'; \qquad (\delta,\ \delta' \text{ entiers conjugués}).$$

Il en résulte

$$-\frac{1}{3}(1 - \alpha\alpha') = (\delta + \delta') + 3\delta\delta' = \text{entier (rationnel)},$$

$$\frac{1}{27}[1 - 3\alpha\alpha' + \alpha\alpha'(\alpha + \alpha')] = \frac{1}{3}(\delta - \delta')^2 + \delta\delta'(\delta + \delta' + 1).$$

Ce dernier terme qui est rationnel est encore un entier car $(\delta - \delta')$ est multiple de $(j - j')$ et son carré est multiple de 3.

4. Les nombres θ_1, θ_2, θ_3 sont indépendants arithmétiquement, sinon il existerait une même relation linéaire, à coefficients entiers (rationnels) entre eux et par suite entre leurs conjugués (obtenus par permutations circulaires) donc entre les termes des colonnes du déterminant constitué ci-dessus; or ceci ne se peut puisque le carré de ce déterminant est $(\alpha\alpha')^2$ qui n'est pas nul.

Je cherche alors la condition pour que le nombre de $\mathbf{R}_\theta$

$$\Im_1 = a\theta_1 + b\theta_2 + c\theta_3 \qquad (a,\ b,\ c \text{ nombres rationnels})$$

soit un entier (de $\mathbf{R}_j$). Il en est de même simultanément des trois conjugués et par suite de leur somme

$$\Im_1 + \Im_2 + \Im_3 = a + b + c,$$

qui doit donc être un entier (rationnel).

Il en est aussi de même de la résolvante de Lagrange dans $\mathbf{R}_{\theta,j}$

$$\Im_1 + j\Im_2 + j'\Im_3 = a\bar{\theta}_1 + b\bar{\theta}_2 + c\bar{\theta}_3 = (a + bj' + cj)\bar{\theta}_1$$

et de son cube qui est dans $\mathbf{R}_j$

$$(\Im_1 + j\Im_2 + j'\Im_3)^3 = (a + bj' + cj)^3\alpha^2\alpha'.$$

Le nombre

$$a + bj' + cj = (b - a)j' + (c - a)j$$

ne peut être une fraction irréductible, car le cube de son dénominateur devrait diviser $\alpha^2\alpha'$, qui, d'après le choix qui a été fait de α, n'a pas de facteur cubique. Il en résulte que

$$a + b + c, \quad b - a, \quad c - a$$

doivent être des entiers rationnels.

Chaque conjugué du nombre considéré peut alors être mis sous la forme

$$\begin{aligned}\Im_u &= a(\theta_u + \theta_{u+1} + \theta_{u+2}) + (b - a)\theta_{u+1} + (c - a)\theta_{u+2},\\ &= a + \eta_u \qquad\qquad (\eta_u \text{ entiers conjugués de } \mathbf{R}_\theta);\end{aligned}$$

leur produit est un polynome en a, dont les coefficients, fonctions symétriques entières des η_u sont des entiers rationnels

$$(a+\eta_1)(a+\eta_2)(a+\eta_3) = a^3 + a^2 e + a e' + e''.$$

Ce produit doit être un entier, *ce qui exige que a et, par suite b et c soient des entiers* (rationnels). Cette condition nécessaire est manifestement suffisante puisque les θ_u sont des entiers (dans $\mathbf{R}_j$); ces θ_u constituent donc bien une base.

5. Parmi les corps ainsi étudiés, les plus simples, qui permettent d'ailleurs d'engendrer tous les autres (§ V) sont ceux dont le discriminant est le carré d'un *nombre premier* (bien entendu congru à $+1$, mod 3).

Je les appelle *corps primaires* (unitaires). En exemples, je donne, pour les premiers d'entre eux (voir le tableau), le discriminant, le couple discriminant unitaire positif, le polynome fondamental du triplet discriminant.

Discriminant : 7^2; couple : $\| -j+2j' \quad -j'+2j \|$; $\alpha+\alpha' = -1$;

$$f(x) = \left(x-\frac{1}{3}\right)^3 - \frac{7}{3}\left(x-\frac{1}{3}\right) + \frac{7}{27} = x^3 - x^2 - 2x + 1.$$

Discriminant : 13^2; couple : $\| -j-4j' \quad -j'-4j \|$; $\alpha+\alpha' = +5$;

$$f(x) = \left(x-\frac{1}{3}\right)^3 - \frac{13}{3}\left(x-\frac{1}{3}\right) - \frac{65}{27} = x^3 - x^2 - 4x - 1.$$

Discriminant : 19^2; couple : $\| 2j+5j' \quad 2j'+5j \|$; $\alpha+\alpha' = -7$;

$$f(x) = \left(x-\frac{1}{3}\right)^3 - \frac{19}{3}\left(x-\frac{1}{3}\right) + \frac{133}{27} = x^3 - x^2 - 6x + 7.$$

Discriminant : 31^2; couple : $\| -j+5j' \quad -j'+5j \|$; $\alpha+\alpha' = -4$;

$$f(x) = \left(x-\frac{1}{3}\right)^3 - \frac{31}{3}\left(x-\frac{1}{3}\right) + \frac{124}{27} = x^3 - x^2 - 10x + 8.$$

Discriminant : 37^2; couple : $\| -4j-7j' \quad -4j'-7j \|$; $\alpha+\alpha' = +11$;

$$f(x) = \left(x-\frac{1}{3}\right)^3 - \frac{37}{3}\left(x-\frac{1}{3}\right) - \frac{407}{27} = x^3 - x^2 - 12x - 11.$$

6. Je passe au cas d'un corps non unitaire; il n'y a plus de base normale et le triplet construit avec le couple générateur n'est plus composé d'entiers. Mais le triple de ce couple, avec une trace nulle, engendre un triplet d'entiers, dont deux d'entre eux constituent, avec 1, une base des entiers du corps. Je précise ces indications par une définition et l'énoncé d'une propriété.

Si un corps abélien n'est pas unitaire, j'appelle couple discriminant le triple du couple générateur, $\|3\alpha \quad 3\alpha'\|$. *et triplet discriminant le système* $\|\theta_1 \quad \theta_2 \quad \theta_3\|$, *construit avec ce couple et une trace nulle.*

Deux nombres (quelconques) *de ce triplet constituent, avec* 1,

$$\| 1 \quad \theta_{u+1} \quad \theta_{u+2} \|, \qquad (u \text{ défini mod } 3),$$

une base des entiers du corps.

En conséquence la valeur du discriminant est

$$\begin{vmatrix} 1 & 1 & 1 \\ \theta_2 & \theta_3 & \theta_1 \\ \theta_3 & \theta_1 & \theta_2 \end{vmatrix}^2 = [(\theta_1 + j\theta_2 + j'\theta_3)(\theta_1 + j'\theta_2 + j\theta_3)]^2 = 9^2(\alpha\alpha')^2;$$

c'est encore le *carré de la norme D du couple discriminant.* Cette norme est le produit de $h-1$ nombres premiers différents, congrus à $+1$, (mod 3) et du nombre 9; inversement le carré d'un tel produit est le discriminant de 2^{h-1} corps non unitaires, engendrés par les divers couples non unitaires dont il est la norme.

Si D est réduit au seul nombre 9 ($h=1$), le couple discriminant, de ce corps appelé $\mathbf{R}_{\theta_0}$, est $\|3j \quad 3j'\|$, le triplet a pour polynome fondamental (§ III, n° 6)

$$f(x) = x^3 - 3x + 1,$$

qui peut être obtenu (*voir* ci-après § VII) en formant l'équation en $x = y + \frac{1}{y}$ de l'équation (en y) aux racines 9e de l'unité.

7. *Les nombres* θ_u *sont bien des entiers,* car leur polynome fondamental (formule 4) qui est

$$f(x) = x^3 - 3\alpha\alpha' x - \alpha\alpha'(\alpha + \alpha'),$$

a ses coefficients entiers rationnels.

Tout nombre de $\mathbf{R}_\theta$ peut être mis sous la forme

$$\vartheta = \frac{a}{3} + \frac{b}{3}\theta_2 + \frac{c}{3}\theta_3, \qquad (a, b, c \in \mathcal{R}).$$

Pour que ce nombre soit entier, il suffit, d'après ce qui vient d'être dit, que a, b, c soient des entiers rationnels, multiples de 3. Je vais montrer que cette condition est nécessaire en établissant des précisions successives sur a, b, c.

Si ϑ est entier, il en est de même de ses conjugués et par suite de leur somme (ou trace commune) qui est dans $\mathcal{R}$

$$\vartheta_1 + \vartheta_2 + \vartheta_3 = a.$$

Il en est encore de même de leur résolvante de Lagrange dans $\mathbf{R}_{\theta,j}$ et de son cube qui est dans $\mathcal{R}$

$$\vartheta_1^3 = (\vartheta_1 + j\vartheta_2 + j'\vartheta_3)^3 = \left(\frac{b}{3}\overline{\theta}_2 + \frac{c}{3}\overline{\theta}_3\right)^3 = \left(\frac{1}{3}\overline{\theta}_1\right)^3 (bj' + cj)^3,$$
$$= \alpha^2\alpha'(bj' + cj)^3 = \alpha^2\alpha' \times \gamma^3.$$

Le nombre γ (de $\mathbf{R}_j$) ne peut être une fraction irréductible, car le cube de son dénominateur devrait diviser $\alpha^2\alpha'$, qui n'a pas de facteur cubique. J'obtiens ainsi la première précision que a, b, c *doivent être des entiers* (rationnels).

Mais je puis construire les $\mathfrak{I}_i$ au moyen de leur trace a et du couple correspondant de $\mathbf{R}_j$ qui est

$$\bar{\mathfrak{I}}^2 : \bar{\mathfrak{I}}' = \left(\gamma\frac{\theta}{3}\right)^2 : \left(\gamma'\frac{\bar{\theta}'}{3}\right) = (\gamma^2:\gamma')\,\alpha, \qquad (\gamma'^2:\gamma)\,\alpha'.$$

Leur polynome fondamental (formule 4) est

$$f(x) = \left(x - \frac{a}{3}\right)^3 - \frac{\alpha\alpha'\gamma\gamma'}{3}\left(x - \frac{a}{3}\right) - \frac{1}{27}\alpha\alpha'(\alpha\gamma^3 + \alpha'\gamma'^3)$$

et il a pour discriminant

$$-\frac{1}{27}(\alpha\alpha')^2(\alpha\gamma^3 - \alpha'\gamma'^3)^2 = -\frac{1}{27}D.$$

J'effectue alors un calcul de congruences dans $\mathbf{R}_j$, (I, 3-c) suivant les puissances du nombre premier $(j-j')$. Les nombres conjugués γ et γ' sont congrus mod$(j-j')$, à un même nombre rationnel e (o ou ± 1): j'en déduis successivement

$$\gamma \equiv \gamma' \equiv e, \quad (\operatorname{mod} j - j'), \qquad \gamma^3 \equiv \gamma'^3 \equiv e^3 \equiv e \quad (\operatorname{mod} 3),$$
$$\alpha\gamma^3 - \alpha'\gamma'^3 \equiv e\,(j - j') \quad (\operatorname{mod} 3), \qquad D \equiv -3e^2 \quad [\operatorname{mod} 3(j - j')].$$

Pour que D soit divisible par $27 = -(j-j')^6$, il est nécessaire que e soit congru à o (mod$j-j'$), donc que les nombres γ et γ' soient divisibles par $(j-j')$. La norme $\gamma\gamma'$ est alors divisible par 3; dans le coefficient de x qui est $\frac{a^2}{3} - \frac{\alpha\alpha'\gamma\gamma'}{3}$, le premier terme doit être aussi entier, de sorte que a^2 et par suite *a doit être divisible par* 3.

Ces précisions montrent que les deux premiers termes (binomes) de $f(x)$ sont à coefficients entiers (rationnels). Il doit en être de même du dernier, ce qui exige

$$\alpha\gamma^3 + \alpha'\gamma'^3 \equiv 0 \qquad [\operatorname{mod} 27 = -(j - j')^6].$$

j'ai déjà obtenu

$$\gamma = (j - j')\gamma_1, \qquad \gamma' = (j' - j)\gamma'_1;$$

et il reste à exprimer

$$\alpha\gamma_1^3 - \alpha'\gamma_1'^3 \equiv 0 \qquad [\operatorname{mod}(j - j')^3].$$

Un calcul analogue au précédent donne

$$\gamma_1 \equiv \gamma'_1 \equiv e_1 \quad (\operatorname{mod} j - j'), \qquad \gamma_1^3 \equiv \alpha'\gamma_1'^3 \equiv e_1^3 \equiv e_1 \quad (\operatorname{mod} 3),$$
$$\alpha\gamma_1^3 - \alpha'\gamma_1'^3 \equiv e_1^3(j - j') \qquad (\operatorname{mod} 3).$$

Il est par suite nécessaire que e_1 soit divisible par $(j-j')$, donc γ, γ' et par suite *b et c doivent être des multiples de* 3.

8. En résumé : **le discriminant d'un corps abélien du 3e degré est le carré d'un nombre entier D produit de facteurs premiers différents, congrus à $+1$, mod 3 et peut être du facteur 9.**

Réciproquement, **si un nombre entier D est produit de h facteurs, dont l'un peut être égal à 9 et les autres nombres premiers différents, congrus à $+1$, mod 3, son carré D^2 est le discriminant de 2^{h-1} corps abéliens du 3e degré.**

9. Il existe des résultats analogues pour les corps du second degré, déterminés comme il a été dit au n° 7 du paragraphe III.

Un corps défini par un entier d (rationnel, positif ou négatif), *sans facteur carré, congru à* $+1$ (mod 4), peut encore être appelé *unitaire; ses entiers ont une base normale* (couple discriminant), (de trace $+1$) qui est

$$\left\| \frac{-1+\sqrt{d}}{2} \quad \frac{-1-\sqrt{d}}{2} \right\|$$

le discriminant est d.

Les premiers d'entre eux sont définis par les discriminants et les polynomes

$$\begin{aligned}
d &= 5, & f(x) &= x^2 - x - 1;\\
d &= -3, & f(x) &= x^2 - x + 1;\\
d &= 13, & f(x) &= x^2 - x - 3;\\
d &= -7, & f(x) &= x^2 - x + 2;
\end{aligned}$$

ces 4 corps sont non seulement unitaires, mais encore *primaires*, les entiers générateurs (égaux aux discriminants) sont premiers (au signe près).

Les corps *non unitaires sont définis par des entiers d, congrus à* -1 *ou à* 2 (mod 4). *Ils ont une base des entiers non normale* (couple discriminant) *qui est* (trace nulle)

$$\| 1 \quad \sqrt{d} \|;$$

le discriminant est 4d.

Il y a trois corps non unitaires, particulièrement simples, définis par les entiers -1 et ± 2, dont les entiers (algébriques) sont (x, y entiers rationnels)

$$\begin{aligned}
&x + yi, && \text{discriminant } -4;\\
&x + y\sqrt{2}, && \text{discriminant } 8;\\
&x + y\sqrt{-2}, && \text{discriminant } -8;
\end{aligned}$$

V. — Composition des corps.

1. Il est possible de construire tous les corps abéliens de degré 3, par une *loi de composition* simple, avec les seuls *corps primaires* (§ IV, n° 5) et avec, en plus, le corps $\mathbf{R}_{0_0}$ de discriminant 9^2 (qui n'est pas unitaire). Ces constructions peuvent être faites, soit avec des triplets quelconques des corps à composer, soit avec les triplets (ou les couples) discriminants. Je précise d'abord le

premier mode, pour deux corps, *a priori* quelconques; dont je supposerai, seulement en explicitant le deuxième mode, que leurs discriminants sont premiers entre eux.

Je note, par un même indice, sans et avec accent $\mathbf{R}_0$ et $\mathbf{R}_{0'}$, les corps engendrés par deux couples (générateurs ou discriminants) conjugués $\|\alpha \quad \alpha'\|$ et $\|\alpha' \quad \alpha\|$, et qui diffèrent par l'ordre des nombres conjugués dans les triplets. Cette notation, comme celle que j'ai employée pour les résolvantes de Lagrange, rappelle le premier élément du couple ou la conjugaison dans $\mathbf{R}_j$.

Dans deux corps abéliens $\mathbf{R}_\xi$ et $\mathbf{R}_\eta$ d'ordre 3, déterminés et ordonnés, *je considère des triplets quelconques, ordonnés à une permutation circulaire près*,

$$\| \xi_1 \quad \xi_2 \quad \xi_3 \|, \qquad \| \eta_1 \quad \eta_2 \quad \eta_3 \|,$$

correspondant respectivement aux couples de $\mathbf{R}_j$

$$\| \beta \quad \beta' \|, \qquad \| \gamma \quad \gamma' \|,$$

sans qu'il soit nécessaire de préciser les traces.

Les triplets ordonnés

$$(5) \qquad \begin{cases} \theta_1 = \xi_1\eta_3 + \xi_2\eta_2 + \xi_3\eta_1 \\ \theta_2 = \xi_1\eta_1 + \xi_2\eta_3 + \xi_3\eta_2 \\ \theta_3 = \xi_1\eta_2 + \xi_2\eta_1 + \xi_3\eta_3 \end{cases} \quad \text{ou} \quad \theta_u = \sum_v (\xi_v \eta_{u-v}); \qquad (u, v, \text{mod } 3);$$

appartiennent à un même corps abélien $\mathbf{R}_0$, *déterminé et ordonné*, que j'appelle *produit des corps considérés*, et que je note

$$\mathbf{R}_0 = \mathbf{R}_\xi \times \mathbf{R}_\eta, \quad \text{ou} \quad \mathbf{R}_{\xi\eta}.$$

(Ce peut être exceptionnellement des triplets de nombres rationnels égaux.)

2. Pour établir cette propriété et justifier la notation, je forme les résolvantes de Lagrange du triplet ainsi construit.

$$\bar\theta_1 = \theta_1 + j\,\theta_2 + j'\theta_3 = \xi_1\bar\eta_3 + \xi_2\bar\eta_2 + \xi_3\bar\eta_1 = \bar\xi_3\bar\eta_1 = \bar\xi_1\bar\eta_3,$$
$$\bar\theta'_1 = \theta_1 + j'\theta_2 + j\,\theta_3 = \xi_1\bar\eta'_3 + \xi_2\bar\eta'_2 + \xi_3\bar\eta'_1 = \bar\xi'_3\bar\eta'_1 = \bar\xi'_1\bar\eta'_3.$$

Ces résolvantes vérifient les relations (2) et (2′) du paragraphe II

$$\begin{aligned} \bar\theta_1^2 : \bar\theta'_1 &= (\bar\xi_3\bar\eta_1)^2 : (\bar\xi'_3\bar\eta'_1) = (\bar\xi_3^2 : \bar\xi'_3)(\bar\eta_1^2 : \bar\eta'_1) = \beta\gamma, \\ \bar\theta'^2_1 : \bar\theta_1 &= (\bar\xi'_3\bar\eta'_1)^2 : (\bar\xi_3\bar\eta_1) = (\bar\xi'^2_3 : \bar\xi_3)(\bar\eta'^2_1 : \bar\eta_1) = \beta'\gamma', \end{aligned} \qquad \bar\theta_1\bar\theta'_1 = \beta\beta'\gamma\gamma'$$

de sorte que le couple correspondant est le *produit* [§ I, n° 6] des couples

$$\| \beta \quad \beta' \| \times \| \gamma \quad \gamma' \| = \| \beta\gamma \quad \beta'\gamma' \|.$$

Si la condition (3) est remplie, c'est-à-dire si $(\beta\gamma)^2(\beta'\gamma')$ n'est pas une puissance cubique exacte, le triplet correspondant est formé des racines d'une équation irréductible.

La trace est le produit des traces

$$\theta_1 + \theta_2 + \theta_2 = \Sigma \xi_u \eta_v = (\Sigma \xi_u)(\Sigma \eta_v); \qquad (u,\ v,\ \text{mod } 3).$$

D'autre part deux triplets ordonnés du corps $\mathbf{R}_\xi$ et deux triplets ordonnés du corps $\mathbf{R}_\eta$ sont définis respectivement par des couples

$$\left\{\begin{matrix} \| \beta_1 \quad \beta'_1 \|, & \| \beta_2 \quad \beta'_2 \|, \\ \| \gamma_1 \quad \gamma'_1 \|, & \| \gamma_2 \quad \gamma'_2 \|, \end{matrix}\right. \quad \text{tels que} \quad \left\{\begin{matrix} (\beta_1^2 \beta'_1):(\beta_2^2 \beta'_2) = \lambda^3, \\ (\gamma_1^2 \gamma'_1):(\gamma_2^2 \gamma'_2) = \mu^3. \end{matrix}\right.$$

La même condition est évidemment remplie par les couples produits

$$[(\beta_1\gamma_1)^2(\beta'_1\gamma'_1)]:[(\beta_2\gamma_2)^2(\beta'_2\gamma'_2)] = (\lambda\mu)^3,$$

de sorte que les triplets correspondants appartiennent au même corps et y ont le même ordre (défini par le couple produit).

3. Si l'ordre est changé dans chacun des corps composants

$$\mathbf{R}_{\xi'} \quad \text{et} \quad \mathbf{R}_{\eta'} \qquad \text{définis par } \| \beta' \quad \beta \| \quad \text{et} \quad \| \gamma' \quad \gamma \|,$$

le corps produit est composé des mêmes nombres, mais avec un ordre différent dans les triplets

$$\mathbf{R}_{\xi'\eta'} \qquad \text{défini par } \| \beta'\gamma' \quad \beta\gamma \|.$$

Si l'ordre est changé dans un seul des corps composants, le corps produit est différent

$$\mathbf{R}_{\xi'\eta} \quad \text{défini par } \| \beta'\gamma \quad \beta\gamma' \| \qquad \text{ou} \qquad \mathbf{R}_{\xi\eta'} \quad \text{défini par } \| \beta\gamma' \quad \beta'\gamma \|.$$

En définitive *deux corps ont deux paires de couples produits*

$$\mathbf{R}_{\xi\eta}, \quad \mathbf{R}_{\xi'\eta'} \qquad \text{et} \qquad \mathbf{R}_{\xi'\eta}, \quad \mathbf{R}_{\xi\eta'};$$

les corps de chaque paire étant égaux, mais avec des ordres différents dans les triplets.

4. Je caractérise maintenant, de façon plus précise, les corps $\mathbf{R}_\xi$ et $\mathbf{R}_\eta$ par leurs *couples discriminants*, que je désigne encore par $\| \beta \quad \beta' \|$ et $\| \gamma \quad \gamma' \|$ et je suppose que les discriminants $(\beta\beta')^2$ et $(\gamma\gamma')^2$ sont premiers entre eux; ceci implique notamment que au plus l'un des corps n'est pas unitaire.

Si deux corps abéliens, de degré 3, *ont des discriminants premiers entre eux, le corps produit a pour couple discriminant le produit des couples discriminants*

$$\left.\begin{matrix} \| \beta \quad \beta' \| \text{ discriminant de } \mathbf{R}_\xi \\ \| \gamma \quad \gamma' \| \text{ discriminant de } \mathbf{R}_\eta \end{matrix}\right\} \qquad \| \beta\gamma \quad \beta'\gamma' \| \text{ discriminant de } \mathbf{R}_{\xi\eta}.$$

Il en résulte notamment que le corps produit est ou n'est pas unitaire, suivant que les deux composants sont unitaires ou que l'un d'eux ne l'est pas.

5. Je distingue les deux cas. *Les deux corps composants sont unitaires.* — Les couples discriminants sont canoniques et unitaires, je les choisis positifs et je considère les triplets discriminants correspondants, de traces égales à $+1$. Le couple produit est encore canonique, unitaire et positif (§ I, n° 6). Le triplet calculé par les formules de multiplication (4) correspond à ce couple, en outre sa trace, produit des traces, est égale à $+1$. C'est le triplet discriminant du corps produit, qui est donc unitaire.

Un seulement des corps est unitaire. — Un des couples discriminants est unitaire, et l'autre est triple d'un couple canonique, non unitaire; je puis les supposer définis par

$$\| 3\beta \quad 3\beta' \|, \qquad \| \gamma \quad \gamma' \|, \qquad \left\{ \begin{matrix} \beta \equiv j, \quad \beta' \equiv j', \\ \gamma \equiv \gamma' \equiv +1, \end{matrix} \right. \qquad (\bmod 3),$$

et je considère les triplets correspondants de traces 0 et $+1$. Le produit des couples est triple d'un couple canonique non unitaire

$$\| 3\beta\gamma \quad 3\beta'\gamma' \|; \qquad \beta\gamma \equiv j, \qquad \beta'\gamma' \equiv j' \qquad (\bmod 3).$$

Le triplet calculé par les formules (5) correspond à ce couple; en outre sa trace, produit des traces est nulle. C'est le triplet discriminant du corps produit qui n'est donc pas unitaire.

6. Ce produit, ou cette composition, peut être étendue à un nombre quelconque de corps dont les discriminants sont premiers entre eux deux à deux (de sorte que l'un d'eux, au plus, n'est pas unitaire).

Inversement en rapprochant ce résultat de ce qui a été dit sur la condition pour qu'un nombre D^2 soit discriminant d'un corps abélien d'ordre 3, j'obtiens la propriété.

Tout corps abélien, d'ordre 3, *est le produit de corps primaires,* dont les discriminants sont des carrés de nombres premiers différents, et peut-être du corps $\mathbf{R}_{0_0}$ dont le discriminant est 9^2.

Cette décomposition n'est possible que d'une seule façon, à condition toutefois de ne pas distinguer des corps $\mathbf{R}_{\xi}$, $\mathbf{R}_{\xi'}$ qui ne diffèrent que par l'ordre adopté pour les nombres conjugués de leurs triplets.

Mais *les produits de h corps primaires,* dont 1 au plus n'est pas unitaire, *sont en nombre* 2^{h-1} ; par exemple pour $c = 3$

$$\mathbf{R}_{\xi\eta\zeta}, \qquad \mathbf{R}_{\xi\eta\zeta'}, \qquad \mathbf{R}_{\xi\eta'\zeta}, \qquad \mathbf{R}_{\xi\eta'\zeta'}.$$

On retrouve ainsi *le nombre* 2^{h-1} *de corps de discriminant égal à* D^2, où D a la forme indiquée.

7. Il existe de même une *composition des corps quadratiques :* aux couples

$$\| \xi_1 \quad \xi_2 \|, \qquad (\xi_1 - \xi_2)^2 = a, \qquad \text{du corps } \mathbf{R}_\xi;$$
$$\| \eta_1 \quad \eta_2 \|, \qquad (\eta_1 - \eta_2)^2 = b, \qquad \text{du corps } \mathbf{R}_\eta;$$

je fais correspondre le couple, défini à une transposition près,

$$\theta_1 = \xi_1\eta_1 + \xi_2\eta_2, \qquad \theta_2 = \xi_1\eta_2 + \xi_2\eta_1, \qquad (\theta_1 - \theta_2)^2 = ab.$$

Ce sont des nombres conjugués d'un corps déterminé (produit)

$$\mathbf{R}_\xi \times \mathbf{R}_\eta \quad \text{ou} \quad \mathbf{R}_{\xi\eta}.$$

Si les deux corps ont leurs discriminants premiers entre eux (un seul au plus étant non unitaire), *le discriminant du corps produit est le produit des discriminants.*

Un corps quadratique est ainsi, d'une et d'une seule façon, le produit de corps primaires et unitaires, de discriminants

$$+p \quad (p \equiv +1, \bmod 4); \qquad -q \quad (q \equiv -1, \bmod 4); \qquad (p, q \text{ premiers})$$

et peut être d'un des trois corps (§ 4, n° 8) de discriminants -4, ou $+8$, ou -8. Son discriminant est :

$$D = \Pi p_i \times \Pi(-q_j) \times \left\{ \begin{array}{c} 1 \\ -4 \\ \text{ou} + 8 \quad \text{ou} - 8. \end{array} \right.$$

VI. — Idéaux d'un corps abélien.

1. Je rappelle sommairement quelques définitions et propriétés de l'arithmétique des idéaux dans un *corps normal* quelconque $\mathbf{R}$, en l'appliquant plus spécialement à un corps abélien $\mathbf{R}_0$ d'ordre 3.

Un idéal $\mathfrak{A}$, *défini par h nombres* ξ_x (de $\mathbf{R}$), *appelés générateurs, est l'ensemble,* désigné par $(\ldots\xi_x\ldots)$, *des nombres*

$$\xi = \sum_x \xi_x \times \text{entier de } \mathbf{R} \qquad (x \text{ de } 1 \text{ à } h).$$

Un générateur peut être remplacé par tout nombre *associé* (produit par un diviseur de 1). Ordinairement un idéal $\mathfrak{A}$ n'est pas nécessairement *principal* (engendré par un seul générateur), on démontre qu'il peut toujours être défini par seulement deux générateurs dont un choisi arbitrairement (dans $\mathfrak{A}$). Un idéal est *entier* si ses générateurs et par suite tous ses nombres sont des entiers (algébriques) de $\mathbf{R}$.

Le *produit de deux idéaux* est l'idéal défini par les produits mutuels des générateurs

$$(\ldots, \xi_x, \ldots) \times (\ldots, \eta_y, \ldots) = (\ldots, \xi_x \eta_y, \ldots) \qquad (x \text{ de } 1 \text{ à } h,\ y \text{ de } 1 \text{ à } k).$$

C'est une opération déterminée (indépendante des systèmes de générateurs), *commutative* et *associative*. L'opération inverse de *division* est possible et déterminée (tout idéal a un inverse).

La *divisibilité des idéaux* (qui remplace celle des facteurs) peut être exprimée par l'une des relations suivantes dont on démontre l'équivalence

$$\mathfrak{M} \text{ multiple de } \mathfrak{D} \ \rightleftharpoons\ \mathfrak{M} \subset \mathfrak{D} \ \rightleftharpoons\ \mathfrak{M} = \mathfrak{D} \times \text{idéal entier}.$$

Il existe des *idéaux premiers* (entiers), chacun n'ayant pour diviseur que lui-même et l'idéal (1). Tout idéal est décomposable d'une et d'une seule façon en un produit de puissances (positives et négatives si l'idéal n'est pas entier) d'idéaux premiers.

Suivant un idéal entier, les entiers de **R** sont répartis en *classes* (de nombres *congrus* entre eux), dont le nombre est la *norme de l'idéal*. La norme d'un produit d'idéaux est le produit des normes. Les classes forment un *anneau* (relativement à l'addition et à la multiplication de leurs termes); cet anneau est un *corps* si l'idéal est premier, et réciproquement.

Un nombre premier rationnel p, considéré comme *base* (ou générateur unique) d'un idéal principal (p), de **R**, est décomposable en un produit de h idéaux premiers $\mathfrak{P}_u$, dont la norme commune est une puissance f de p, appelée degré de l'idéal $\mathfrak{P}_u$

$$(p) = \mathfrak{P}_1 \times \mathfrak{P}_2 \times \ldots \times \mathfrak{P}_h, \qquad [N(\mathfrak{P}_u) = p^f;\ hf = \text{degré de } \mathbf{R}].$$

Dans chaque idéal $\mathfrak{P}_u$, p est le p. g. c. d. des entiers rationnels qu'il contient.

Pour un corps abélien de degré 3, il y a ainsi deux espèces de nombres premiers (rationnels), suivant leur décomposition

$$(p) = \mathfrak{P}_1 \times \mathfrak{P}_2 \times \mathfrak{P}_3, \qquad N(\mathfrak{P}_u) = p;$$

et

$$(q) = \mathfrak{Q}, \qquad N(\mathfrak{Q}) = q^3.$$

Les idéaux conjugués, diviseurs de p peuvent être définis par deux générateurs, l'un commun qui est p, les autres respectivement conjugués

$$\mathfrak{P}_u = (p, \omega_u); \qquad (\text{pour } \mathbf{R}_0\text{: } u \text{ défini mod } 3).$$

2. La décomposition d'un nombre premier (rationnel), ou la recherche des idéaux premiers dans un corps $\mathbf{R}_0$ peut être réalisée d'une première façon, en utilisant le *couple discriminant* $\| \alpha \quad \alpha' \|$ (défini à l'ordre près).

1° *Si un nombre premier p n'est pas diviseur de la racine carrée D du discriminant* (norme du couple discriminant) d'un corps abélien $\mathbf{R}_0$ d'ordre 3, *il n'est divisible que par des idéaux premiers distincts* (à la puissance 1).

Dans ce cas, suivant que la congruence (dans $\mathbf{R}_j$)

$$(6) \qquad y^3 - \alpha^2\alpha' \equiv 0 \quad \begin{cases} (\text{mod } p), \text{ si } p \neq 3, \\ (\text{mod } p^2), \text{ si } p = 3; \end{cases}$$

est impossible ou possible, (p) *est un idéal premier* (de degré 3), *ou produit de trois idéaux premiers conjugués* (différents, de degré 1).

2° *Si p est diviseur de* D, *il est le cube d'un idéal premier* (du premier degré).

3. La première Partie de 1° peut être établie pour tout corps de nombres algébriques (même non normal). J'en donne, dans le cas considéré, une démonstration directe (par l'absurde) en utilisant le triplet discriminant et ses résolvantes de Lagrange.

Je suppose (p) divisible par le carré $\mathfrak{T}^2$ d'un idéal premier, il est alors produit de trois idéaux conjugués, que je puis définir par deux générateurs, p commun et trois entiers conjugués

$$p = \mathfrak{T}_1 \times \mathfrak{T}_2 \times \mathfrak{T}_3; \qquad \mathfrak{T}_1 = (p, \omega_1), \qquad \mathfrak{T}_2 = (p, \omega_2), \qquad \mathfrak{T}_3 = (p, \omega_3).$$

Deux d'entre eux sont égaux à $\mathfrak{T}$; l'égalité $\mathfrak{T} = \mathfrak{T}_u = \mathfrak{T}_{u+1}$ entraîne l'existence d'entiers ξ_u, η_v de $\mathbf{R}_j$, tels que

$$\omega_{u+1} = p\xi_u + \omega_u \eta_u;$$

cette relation entraîne la relation conjuguée (substitution de $u+1$ à u)

$$\omega_{u+2} = p\xi_{u+1} + \omega_{u+1}\eta_{u+1};$$

ce qui exprime l'égalité de $\mathfrak{T}_{u+2}$ et de $\mathfrak{T}_{u+1}$, de sorte que $(p) = \mathfrak{T}^3$.

Suivant cet idéal unique $\mathfrak{T}$ (de norme p), les entiers de $\mathbf{R}_0$ sont répartis en p classes qui peuvent être définies (comme pour $\mathbf{R}_j$, § I, n° 3) par des représentants rationnels (définis mod p). Les entiers θ_u du triplet discriminant appartiennent à une même classe a (rationnel), car si $\theta_1 - a$ est dans l'idéal $\mathfrak{T}$, il en est de même de ses conjugués $\theta_2 - a$ et $\theta_3 - a$. Il en résulte, dans le corps $\mathbf{R}_{0,j}$, les congruences

$$\begin{aligned} \bar{\theta}_1 &= (\theta_1 - a) + j(\theta_2 - a) + j'(\theta_3 - a) \equiv 0, \\ \bar{\theta}'_1 &= (\theta_1 - a) + j'(\theta_2 - a) + j(\theta_3 - a) \equiv 0, \end{aligned} \qquad (\text{mod } \bar{\mathfrak{T}});$$

et, *a fortiori*,

$$D = \alpha\alpha' = \bar{\theta}_1\bar{\theta}'_1 \equiv 0, \qquad (\text{mod } \bar{\mathfrak{T}}).$$

L'idéal $\bar{\mathfrak{T}}$, dans $\mathbf{R}_{0,j}$ (entier, mais non nécessairement premier) est obtenu en multipliant par tous les entiers de $\mathbf{R}_j$ tous les nombres de $\mathfrak{T}$, ce qui ne change pas l'ensemble de ceux qui sont rationnels, ni leur p. g, c. d. qui est p, lequel divise donc D.

4. *Condition nécessaire de décomposition de p* (ou preuve par l'absurde de la condition suffisante d'impossibilité de la congruence). Je suppose (p) divisible par un idéal $\mathfrak{T}$ du premier degré. Les nombres θ_1, θ_2, θ_3 du triplet discriminant sont respectivement congrus, mod $\mathfrak{T}$, à des entiers rationnels a_1, a_2, a_3; il en résulte la congruence, dans $\mathbf{R}_{0,j}$

$$a_1 + ja_2 + j'a_3 \equiv \theta_1 + j\theta_2 + j'\theta_3, \qquad (\text{mod } \overline{\mathfrak{T}});$$

et, *par élévation au cube*, et tenant compte d'une des relations (2′)

$$(a_1 + ja_2 + j'a_3)^3 - \alpha^2\alpha' \equiv 0, \qquad (\text{mod } \overline{\mathfrak{T}}). \tag{6'}$$

J'ai dit que les nombres de $\overline{\mathfrak{T}}$ sont de la forme

$$\xi \times \delta; \qquad [\xi \in \mathfrak{T}, \ \delta \text{ entier de } \mathbf{R}_j];$$

ceux qui sont dans $\mathbf{R}_j$ sont nécessairement obtenus avec des nombres ξ de $\mathfrak{T}$, également dans $\mathbf{R}_j$ et par conséquent rationnels; ce sont par suite des produits de p par des entiers de $\mathbf{R}_j$. Le premier membre de la congruence (6′) étant dans $\mathbf{R}_j$, elle est donc encore vraie pour le module p; ce qui démontre la possibilité de la congruence (6) de l'énoncé pour tout nombre premier p décomposable (ceci est valable dans le cas de facteurs non distincts).

Dans le cas de $p = 3$, l'élévation au cube permet de remplacer mod $\overline{\mathfrak{T}}$, par mod $\overline{\mathfrak{T}}^2$. En effet l'égalité

$$\bar{\theta}_1 = \gamma + \bar{\xi}, \qquad (\gamma \text{ entier de } \mathbf{R}_j, \qquad \bar{\xi} \in \overline{\mathfrak{T}})$$

entraîne, en tenant compte des valeurs des coefficients du binome,

$$\bar{\theta}_1^3 = \gamma^3 + 3\bar{\eta} + \bar{\xi}^3, \qquad [3, \ \bar{\eta}, \ \bar{\xi} \in \overline{\mathfrak{T}}; \qquad 3\bar{\eta} + \bar{\xi}^3 \in \overline{\mathfrak{T}}^2].$$

Je suppose cette fois, explicitement, 3 non divisible par $\overline{\mathfrak{T}}^2$, tout entier rationnel, divisible par $\overline{\mathfrak{T}}^2$, l'est donc aussi par 3^2; un raisonnement analogue au précédent montre que tout entier de $\overline{\mathfrak{T}}^2$ qui appartient à $\mathbf{R}_j$ est nécessairement divisible par 3^2; il en est ainsi du premier membre de (6′), ce qui établit le deuxième cas de la condition nécessaire de décomposition.

5. *Condition suffisante de décomposition de p.* — Je suppose possible la congruence de l'énoncé; j'appelle encore $\| \theta_1 \ \theta_2 \ \theta_3 \|$ le triplet discriminant et $f(x)$ son polynome fondamental. Je vais montrer, en distinguant trois cas, l'existence d'un entier (rationnel) c, annulant $f(x)$, relativement au module p

$$f(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3); \qquad f(c) \equiv 0, \qquad (\text{mod } p).$$

a. Le corps est unitaire et $p \neq 3$; je considère une solution γ de la congruence, γ' l'entier conjugué (dans $\mathbf{R}_j$) et je détermine l'entier rationnel c par les conditions ($s = +1$)

$$\gamma^3 \equiv \alpha^2\alpha'; \qquad \gamma\gamma' \equiv \alpha\alpha'; \qquad 3c \equiv \gamma + \gamma' + 1, \qquad (\text{mod } p).$$

Le calcul d'élimination fait ci-dessus (§ II, n° 4 et § IV, n° 3) montre que

$$(7\text{-}a) \qquad 27f(c) = (3c-1)^3 - 3\alpha\alpha'(3c-1) - \alpha\alpha'(\alpha+\alpha') \equiv 0 \qquad (\text{mod } p)$$

et je puis diviser le premier membre par 27, qui est premier avec p.

b. Le corps est unitaire et $p = 3$. Je détermine cette fois les entiers conjugués γ, γ' de $\mathbf{R}_j$ par les congruences

$$\gamma^3 \equiv \alpha^2\alpha', \qquad \gamma\gamma' \equiv \alpha\alpha', \qquad (\text{mod } 81).$$

Pour le faire, à partir d'une solution γ_1 de la congruence (6), je détermine successivement $\gamma_2 = \gamma_1 + 3x$ et $\gamma = \gamma_2 + 9y$, puis γ' conjugué de γ, par les congruences

$$(\gamma_1 + 3x)^3 - \alpha^2\alpha' \equiv 0 \quad (\text{mod } 27) \qquad \text{ou} \qquad \frac{\gamma_1^3 - \alpha^2\alpha'}{9} + x\gamma_1^2 \equiv 0 \quad (\text{mod } 3);$$

$$(\gamma_2 + 9y)^3 - \alpha^2\alpha' \equiv 0 \quad (\text{mod } 81) \qquad \text{ou} \qquad \frac{\gamma_2^3 - \alpha^2\alpha'}{27} + y\gamma_2^2 \equiv 0 \quad (\text{mod } 3);$$

elles sont possibles, puisque

$$\alpha^2\alpha' \not\equiv 0, \qquad \gamma_1 \not\equiv 0, \qquad \gamma_2 \equiv \gamma_1 \not\equiv 0, \qquad \gamma \equiv \gamma_2 \not\equiv 0 \qquad (\text{mod } 3).$$

Il en résulte

$$\gamma^3 + \gamma'^3 \equiv \alpha\alpha'(\alpha + \alpha'), \qquad (\text{mod } 81);$$
$$\gamma + \gamma' \equiv \gamma^3 + \gamma'^3 \equiv \alpha\alpha'(\alpha+\alpha') \equiv -1, \qquad (\text{mod } 3).$$

Je détermine l'entier rationnel c par la congruence

$$3c \equiv \gamma + \gamma' + 1, \quad (\text{mod } 81), \qquad \text{ou} \qquad c \equiv \frac{\gamma + \gamma' + 1}{3}, \quad (\text{mod } 27).$$

Un calcul analogue au précédent montre que

$$(7\text{-}b) \qquad \begin{aligned} 0 &\equiv (3c-1)^3 - (\gamma+\gamma')^3, \\ &\equiv (3c-1)^3 - 3\alpha\alpha'(3c-1) - \alpha\alpha'(\alpha+\alpha') \equiv 27f(c), \end{aligned} \qquad (\text{mod } 81),$$

et je puis supprimer le coefficient 27, en remplaçant le module 81 par 3.

c. Le corps n'est pas unitaire et p est différent de 3, puisqu'il ne divise pas le discriminant. A partir d'une solution γ de la congruence, je détermine cette fois l'entier c par les conditions

$$\gamma^3 \equiv \alpha^2\alpha', \qquad \gamma\gamma' \equiv \alpha\alpha', \qquad c \equiv 3\gamma + 3\gamma', \qquad (\text{mod } p).$$

Le calcul d'élimination (§ II, n° 4 et § IV, n° 6) montre que

$$(7\text{-}c) \qquad 0 \equiv c^3 - 3\alpha\alpha' c - \alpha\alpha'(\alpha+\alpha') \equiv f(c), \qquad (\text{mod } p)$$

6. La congruence ainsi établie dans les trois cas (7-a, 7-b, 7-c) et considérée dans $\mathbf{R}_0$

$$(c-\theta_1)(c-\theta_2)(c-\theta_3)\equiv 0, \qquad (\text{mod } p). \tag{7}$$

montre que l'idéal (p) a, avec au moins l'un des facteurs du premier membre, un diviseur commun, différent de (1)

$$\mathfrak{P}_u=(p,\ c-\theta_u),$$

et ceci affirme la décomposition de (p). Chacun des idéaux

$$\mathfrak{P}_1=(p,\ c-\theta_1), \qquad \mathfrak{P}_2=(p,\ c-\theta_2), \qquad \mathfrak{P}_3=(p,\ c-\theta_3)$$

est d'ailleurs différent de (1); sinon il existerait une relation

$$\alpha_v p+\beta_v(c-\theta_v)=1 \qquad (\alpha_v,\ \beta_v \text{ entiers de } \mathbf{R}_0),$$

qui, étant vérifiée pour une valeur de v, devrait l'être aussi pour les deux autres valeurs, de sorte que les trois idéaux seraient égaux à (1), ce qui est absurde.

Les nombres p, $c-\theta_1$, $c-\theta_2$, $c-\theta_3$, sont premiers entre eux; sinon il y aurait dans $\mathbf{R}_{0,j}$ un facteur (idéal) commun à

$$p, \qquad [(\theta_1-c)+j(\theta_2-c)+j'(\theta_3-c)]=\bar{\theta}, \qquad [(\theta_1-c)+j'(\theta_2-c)+j(\theta_3-c)]=\bar{\theta}';$$

et *a fortiori* un facteur commun à

$$p \quad \text{et} \quad \bar{\theta}\bar{\theta}'=\alpha\alpha';$$

qui sont des nombres premiers entre eux.

Ceci acquis, si (p) n'a pas de diviseur commun avec deux des facteurs c'est-à-dire si

$$(p,\ c-\theta_u,\ c-\theta_v)=1, \qquad \text{pour} \quad u\neq v;$$

les trois idéaux $\mathfrak{P}_u=(p,\ c-\theta_u)$ sont premiers entre eux deux à deux; donc (p) est divisible par leur produit et l'égalité des normes montre que cette divisibilité est une égalité.

Si l'idéal

$$\mathfrak{P}_u=(p,\ c-\theta_{u+1},\ c-\theta_{u+2})$$

est différent de (1), il en est de même des trois conjugués (définis par les trois valeurs de u). Ces conjugués sont premiers entre eux, donc distincts et (p) est égal à leur produit. Ce deuxième cas présente un caractère exceptionnel, il ne se produit que si p divise les différences $\theta_{u+1}-\theta_{u+2}$ et par suite le discriminant des θ_u $\left[\text{sans diviser celui du corps, c'est-à-dire encore si } p \text{ divise } \frac{(\alpha-\alpha')^2}{3}\right]$.

7. *Décomposition d'un diviseur du discriminant.* — Je considère enfin un nombre premier p diviseur du discriminant D (du corps); je vais d'abord

montrer, en distinguant encore 3 cas, que le polynome $f(x)$, fondamental du triplet, se réduit, suivant le module p à

$$f(x) \equiv (x-c)^3, \quad (\bmod p); \qquad [c \text{ entier rationnel}].$$

a. Le corps est unitaire, p est alors diviseur de $\alpha\alpha'$ et différent de 3, de sorte que

$$27 f(x) \equiv (3x-1)^3 \equiv 27(x-c)^3, \qquad (\bmod p); \tag{8-a}$$

c désignant l'inverse de 3, $(\bmod p)$.

b. Le corps n'est pas unitaire et p est différent de 3; il est encore diviseur de $\alpha\alpha'$ et le polynome se réduit à

$$f(x) \equiv x^3 \equiv (x-c)^3, \qquad (\bmod p). \tag{8-b}$$

c. Le corps n'est pas unitaire et $p=3$. Tenant compte des coefficients du binome et du théorème de Fermat, le polynome peut être réduit à

$$f(x) \equiv x^3 - \alpha\alpha'(\alpha+\alpha') \equiv (x-c)^3, \qquad (\bmod 3), \tag{8-c}$$

c étant congru $(\bmod 3)$ au nombre rationnel $\alpha\alpha'(\alpha+\alpha')$, donc à ± 1.

Dans les trois cas la substitution d'un nombre θ_u du triplet dans le polynome donne la congruence

$$(\theta_u - c)^3 \equiv 0, \qquad (\bmod p). \tag{8}$$

Tous les facteurs premiers éventuels de (p) sont diviseurs, à la fois, des 3 valeurs de $(\theta_u - c)$, donc de l'idéal

$$\mathfrak{L} = (p, \theta_1 - c, \theta_2 - c, \theta_3 - c),$$

qui est différent de (1). Relativement à cet idéal, pris pour module, les congruences

$$c \equiv \theta_1 \equiv \theta_2 \equiv \theta_3 \qquad (\bmod \mathfrak{L})$$

montrent que tout entier de $\mathbf{R}_0$, qui est de la forme $u\theta_1 + v\theta_2 + w\theta_3$ (u, v, w entiers rationnels) est congru à un entier rationnel, défini $\bmod p$. Il y a donc p classes, relativement à $\mathfrak{L}$ qui est par suite un idéal du premier degré, de norme p, et premier. C'est le seul facteur premier de (p) et l'égalité des normes montre que

$$(p) = \mathfrak{L}^3.$$

8. Les conditions ainsi obtenues de décomposition d'un nombre premier rationnel p, dans un corps abélien du troisième ordre, ne font intervenir que le couple discriminant, considéré au module p, ou éventuellement au module 9, près. Cette remarque peut être précisée par l'énoncé suivant :

La qualité d'un nombre premier p d'être un idéal premier, ou un produit de 3 idéaux premiers distincts, ou une puissance cubique d'idéal premier, est la même pour tous les corps abéliens, d'ordre 3, **dont les couples discriminants** (dans $\mathbf{R}_j$) **sont congrus** (mod p), si $p \not\equiv 3$, **ou modulé** p^2, si $p = 3$.

Je complète ci-après (§ VIII) ce premier résultat par une **loi de réciprocité** qui permet d'affirmer que la qualité de décomposition est aussi la même, dans un corps donné, pour tous les nombres premiers congrus entre eux suivant le discriminant, pris pour module.

9. En vue de la recherche des corps dans lesquels un nombre premier donné a une qualité déterminée, je précise les propriétés déjà données (§ I, n° 3) de la répartition en classes, suivant un module premier, dans $\mathbf{R}_j$, en indiquant celles de ces classes qui sont des puissances cubiques.

a. Module : idéal premier (q) *du second degré* ($q \equiv -1$, mod 3; $q^2 - 1$ classes premières avec q). Celles des classes qui sont puissances cubiques sont définies par

$$\gamma^{3y}, \quad (\bmod q); \qquad \begin{cases} \gamma \text{ racine primitive;} \\ y \text{ défini } \left[\bmod (q-1)\dfrac{q+1}{3}\right]; \end{cases}$$

elles comprennent les $q-1$ classes à représentant rationnel. Pour que le nombre $\alpha^2\alpha' = \mathrm{N}(\alpha)\alpha$ soit congru (mod q) à une puissance cubique, il faut et il suffit qu'il en soit de même de α. Les classes de couples discriminants des corps dans lesquels q est décomposable sont donc définies par

$$\alpha \equiv \gamma^{3y}, \qquad (\bmod q);$$

elles sont en nombre $(q-1)\dfrac{q+1}{3}$.

b. Module : nombre premier p décomposable [$p \equiv +1$ (mod 3); $(p-1)^2$ classes premières avec p]. — Le groupe de ces classes étant défini par deux générateurs conjugués γ, γ', les couples d'indices de deux nombres conjugués α et α' se déduisent par transposition des exposants

$$\alpha \equiv \gamma^x\gamma'^y, \qquad \alpha' \equiv \gamma^y\gamma'^x, \qquad (\bmod p),$$

de sorte que

$$\alpha^2\alpha' \equiv \gamma^{2x+y}\gamma'^{x+2y} \quad (\bmod p).$$

Pour que ce nombre soit puissance cubique, il faut et il suffit que les exposants soient divisibles par 3, ce qui est équivalent à $x \equiv y$ (mod 3). Les classes des couples discriminants des corps dans lesquels p est décomposable peuvent ainsi être définies par

$$\alpha \equiv \gamma^x\gamma'^{x+3z} \qquad (\bmod p);$$

Il suffit de donner à x les valeurs de 1 à $p-1$ et à z les valeurs de 1 à $\frac{p-1}{3}$; les classes sont donc en nombre $(p-1)\frac{p-1}{3}$.

c. Module 3. — Je cherche la condition pour que $\alpha^2\alpha'$ soit congru à une puissance cubique (mod 9). En y ajoutant la condition que le corps doit être unitaire c'est-à-dire $\alpha \equiv \alpha' \equiv +1 \pmod 3$, j'obtiens les seules classes $\alpha \equiv \alpha' \equiv +1 \pmod 9$.

10. Les conditions de décomposition d'un nombre premier, en idéaux premiers, dans un corps quadratique sont bien connues et se rattachent à l'étude des congruences du second degré. Elles peuvent être exprimées par un énoncé analogue à celui qui a été donné ci-dessus pour les corps abéliens du troisième degré et qui pourrait être établi de la même façon :

Dans un corps quadratique :

1° *Si un nombre premier p n'est pas diviseur du discriminant D il n'est divisible que par des idéaux premiers distincts; dans ce cas, suivant que la congruence* (dans $\mathcal{R}$)

$$y^2 - D \equiv 0 \quad \begin{cases} \pmod p, \text{ si } p \neq 2; \\ \pmod{p^2}, \text{ si } p = 2 \end{cases}$$

est impossible, ou possible, p est un idéal premier (de degré 2) *ou il est décomposable en un produit de* 2 *idéaux premiers* (conjugués) *distincts.*

2° *Si p est diviseur de D, il est le carré d'un idéal premier, du premier degré* (égal à son conjugué).

Cet énoncé met en lumière le rôle spécial de 2 pour les corps quadratiques, analogue au rôle spécial de 3 pour les corps abéliens du troisième degré. Il en résulte encore la remarque :

La qualité d'un nombre premier, d'être un idéal premier, ou un produit de deux idéaux premiers distincts, ou le carré d'un idéal premier, *est la même pour tous les corps quadratiques, dont les discriminants sont congrus, mod* p *si p est impair, ou mod* p^2 *si* $p = 2$.

VII. — Sous-corps des corps circulaires.

1. J'ai construit jusqu'ici un corps abélien par une opération algébrique nouvelle, dans le corps $\mathbf{R}_j$, en l'espèce la racine cubique d'un nombre $\alpha^2\alpha'$. Je vais maintenant le constituer par un choix convenable d'éléments dans un corps supposé connu, en l'espèce un corps circulaire (de racines convenables de l'unité). Je précise cette indication par un énoncé général.

Un corps abélien $\mathbf{R}_\theta$, d'ordre 3, *de discriminant* D^2, [D produit de nombres premiers différents, congrus à $+1$ (mod 3) et éventuellement d'un facteur 9], *est sous-corps du corps circulaire* $\mathbf{R}_{(D)}$, *des racines d'indice* D *de l'unité*, de degré $\varphi(D) = N$.

Son triplet discriminant est constitué, au signe près, *par* 3 *sommes de racines primitives*, réparties par un groupe quotient $\mathbf{G}_S \mid \mathbf{G}_s$ d'ordre 3, du groupe de Galois $\mathbf{G}_S$ de $\mathbf{R}_D$

$$(9) \qquad \theta_1 = \sum_x \varepsilon_D.(s_x), \qquad \theta_2 = \sum_x \varepsilon_D.(\sigma \times s_x), \qquad \theta_3 = \sum_x \varepsilon_D.(\sigma^2 \times s_x),$$

ε_D racine primitive d'indice D de l'unité; $\mathbf{G}_S$ groupe de Galois de $\mathbf{R}_D$; $\mathbf{G}_s$ sous-groupe d'index 3 [*voir* ci-après § VIII, n° 2] de substitutions s_x; (σ), (σ^2), $(\sigma^3) = 1$, substitutions des classes de $\mathbf{G}_S \mid \mathbf{G}_s$.

Le choix d'un ordre [(σ), (σ^2), (σ^3) ou (σ^2), $(\sigma^4) = (\sigma)$, $(\sigma^6) = 1$] dans le groupe quotient détermine un ordre, à une permutation circulaire près, des nombres dans les triplets du corps $\mathbf{R}_\theta$.

Les trois sommes (appelées aussi *périodes de Gauss*) sont respectivement invariantes pour $\mathbf{G}_s$ et permutées circulairement par $\mathbf{G}_S$. Je vais établir la propriété d'abord pour des *corps primaires* (D premier, ou égal à 9); je l'étendrai ensuite au cas général, en utilisant l'opération de composition ou de multiplication des corps (§ V).

2. Pour *le corps* $\mathbf{R}_{\theta_0}$, *de couple discriminant* $\| 3j \quad 3j' \|$ la propriété a déjà été signalée (§ IV, n° 6). Les nombres du triplet discriminant sont donnés par les sommes

$$\theta_1 = \varepsilon + \varepsilon^{-1}, \qquad \theta_2 = \varepsilon^2 + \varepsilon^{-2}, \qquad \theta_3 = \varepsilon^4 + \varepsilon^{-4},$$

où ε est une racine (quelconque) du polynome

$$\theta_2(x) = x^6 + x^3 + 1.$$

Les racines de ce polynome sont les *racines primitives* 9[ièmes] *de l'unité* et définissent le corps $\mathbf{R}_{(9)}$; le groupe de ce corps est cyclique et isomorphe au groupe multiplicatif des 6 classes (mod 9), premières avec 9. Ses substitutions peuvent être définies par

$$\varepsilon.(S_X) = \varepsilon^{2^X}; \qquad [2^X, (\text{mod } 9); \quad X, (\text{mod } 6)].$$

Le sous-groupe $\mathbf{G}_s$, d'index 3 et d'ordre 2 est formé des substitutions, puissance cubiques

$$(S_3) = (s_1), \quad (S_6) = (s_2) = 1; \qquad [\varepsilon.(s_1) = \varepsilon^{-1}, \quad \varepsilon.(s_2) = \varepsilon];$$

les trois classes du groupe quotient $\mathbf{G}_S \mid \mathbf{G}_s$ sont

$$(S_3), \quad (S_6) = 1; \qquad (S_2), \quad (S_5); \qquad (S_4), \quad (S_1).$$

Leur ordre entraîne celui des θ_u et par suite celui des nombres de tout triplet de $\mathbf{R}_{\theta_0}$, à une permutation circulaire près. Elle entraîne par suite l'ordre du couple discriminant qui peut être calculé directement en formant les carrés des résolvantes

$$\begin{aligned}\bar\theta^2 &= [\varepsilon+\varepsilon^{-1}+j(\varepsilon^2+\varepsilon^{-2})+j'(\varepsilon^4+\varepsilon^{-4})]^2\\ &= 3[\varepsilon^2+\varepsilon^{-2}+j'(\varepsilon^4+\varepsilon^{-4})+j(\varepsilon+\varepsilon^{-1})] = 3j'\bar\theta';\end{aligned}$$
$$\bar\theta^2 : \bar\theta' = 3j'; \qquad \bar\theta'^2 : \bar\theta = 3j.$$

3. Pour constituer un *corps primaire* (unitaire) de discriminant P^2, carré d'un nombre premier P, congru à $+1$ (mod 3), je considère le corps $\mathbf{R}_{(P)}$ des racines, d'indice P, de l'unité, d'ordre $N = P - 1$. Son groupe $\mathbf{G}_S$ est cyclique et isomorphe au groupe multiplicatif des classes (mod P) premières avec P, engendré par une classe primitive g; ses substitutions peuvent être définies par

$$\varepsilon.(S_X) = \varepsilon^{g^X} \qquad [g^X, \text{ mod } P; \quad X, \text{ mod } N].$$

Le nombre N est, par hypothèse, divisible par 3, le groupe $\mathbf{G}_S$ a un et un seul sous-groupe (d'index 3 et d'ordre $N:3$), constitué par les substitutions qui sont puissances cubiques $(s_x) = (S_{3x})$. Je désigne par (σ), (σ^2), $(\sigma^3) = 1$ des représentants des classes du groupe quotient $\mathbf{G}_S | \mathbf{G}_s$, de sorte que

$$\varepsilon.(s_x) = \varepsilon^{g^{3x}}, \qquad \varepsilon.(\sigma\times s_x) = \varepsilon^{g^{3x'+1}}, \qquad \varepsilon.(\sigma^2\times s_x) = \varepsilon^{g^{3x''+2}}.$$

Je forme les sommes des formules (9) de l'énoncé général, puis leurs résolvantes de Lagrange, qui, *a priori*, sont dans le corps $\mathbf{R}_{(P),j} = \mathbf{R}_{(3P)}$

$$\bar\theta = \sum_x \{\varepsilon.(s_x) + j[\varepsilon.(\sigma\times s_x)] + j'[\varepsilon.(\sigma^2\times s_x)]\},$$
$$\bar\theta' = \sum_x \{\varepsilon.(s_x) + j'[\varepsilon.(\sigma\times s_x)] + j[\varepsilon.(\sigma^2\times s_x)]\}.$$

Une substitution quelconque (s_x) de $\mathbf{G}_S$ les laissent invariantes, une substitution (σ) ou (σ^2) les multiplie par j ou j' (ou encore change l'indice des résolvantes)

$$\bar\theta.(s_x) = \bar\theta, \qquad \bar\theta.(\sigma\times s_x) = j'\bar\theta, \qquad \bar\theta.(\sigma^2\times s_x) = j\bar\theta,$$
$$\bar\theta'.(s_x) = \bar\theta', \qquad \bar\theta'.(\sigma\times s_x) = j\bar\theta', \qquad \bar\theta'.(\sigma^2\times s_x) = j'\bar\theta'.$$

Le raisonnement déjà fait (§ II, n° 5) montre que les quotients

$$\bar\theta^2 : \bar\theta' = \alpha, \qquad \bar\theta'^2 : \bar\theta = \alpha',$$

qui sont invariables pour toute substitution $(S) = (\sigma^u \times s_x)$, du groupe $\mathbf{G}_S$ [du corps $\mathbf{R}_{(P)}$], ont leurs valeurs dans $\mathbf{R}_j$ et y sont conjugués, puisqu'elles sont transposées par transposition de j et j'. Reste à préciser la valeur du couple $\|\alpha \quad \alpha'\|$.

4. *Norme du couple.* — La norme du couple est le produit des résolvantes [relation (2′)]

$$\alpha\alpha' = \bar{\theta}\bar{\theta}' = (\theta_1 + j\theta_2 + j'\theta_3)(\theta_1 + j'\theta_2 + j\theta_3) = (\theta_1^2 + \theta_2^2 + \theta_3^2) - (\theta_2\theta_3 + \theta_3\theta_1 + \theta_1\theta_2).$$

Chaque parenthèse est invariante pour toute substitution de $\mathbf{G}_S$, sa valeur est par suite rationnelle. D'autre part c'est une expression linéaire de racines primitives ε^{g^x}; chacune renferme donc éventuellement un certain nombre de termes $+1$ et le même nombre de fois chacune des racines primitives. Cette remarque en permet le calcul par énumération.

Dans chaque θ_u, les racines ε peuvent être réparties par couples d'inverses correspondant aux substitutions

$$(S_X) \text{ définie par } g^X; \quad (S_X \times s_{N:6}), \text{ définie par } g^{X+3(N:6)};$$

puisque

$$g^{X+3(N:6)} \equiv (g^X)(g^{N:2}) \equiv -g^X \qquad (\text{mod } P).$$

Dans chaque carré θ_u^2, il y a donc $(N:3)$ termes $+1$; dans la première parenthèse, il y en a N; les autres termes, en nombre

$$3(N:3)^2 - N = \frac{N^2}{3} - N = N\left(\frac{N}{3} - 1\right),$$

sont des racines primitives et chacune d'elles est répétée $\left(\frac{N}{3} - 1\right)$ fois. La somme de ces racines étant -1, la valeur de cette première parenthèse est

$$(+1)N + (-1)\left(\frac{N}{3} - 1\right) = \frac{2N}{3} + 1.$$

Dans chaque produit $\theta_u\theta_{u+1}$, il n'y a que des produits de racines non inverses, tous les termes sont donc des racines primitives, leur nombre total est $3\left(\frac{N}{3}\right)^2 = \frac{N}{3}N$, de sorte que chacune d'elles est répétée $\frac{N}{3}$ fois. La somme des deux parenthèses, qui est la norme cherchée, est

$$\alpha\alpha' = \frac{2N}{3} + 1 - \left(\frac{N}{3}\right)(-1) = N + 1 = P.$$

5. *Le couple est formé d'entiers.* — La norme ainsi calculée étant un entier, il suffit de prouver que la trace est aussi un entier. La valeur de cette trace est

$$\alpha + \alpha' = (\bar{\theta}^2 : \bar{\theta}') + (\bar{\theta}'^2 : \bar{\theta}) = (\bar{\theta}^3 + \bar{\theta}'^3) : \bar{\theta}\bar{\theta}' = (\bar{\theta}^3 + \bar{\theta}'^3) : P.$$

La dernière parenthèse dont la valeur est, *a priori*, dans $\mathbf{R}_{(3P)}$ est invariante pour toute substitution (S_X) et pour la transposition de j et j'; c'est donc un nombre rationnel (dans $\mathcal{R}$) qui, d'après sa construction (fonction entière d'entiers algébriques), est entier. Il suffit d'établir qu'il est divisible par P.

Or je puis écrire l'expression de $\overline{\theta}$

$$\overline{\theta} = \bar{\theta} - \frac{N}{3}(1+j+j') = \left[\left(\theta_1 - \frac{N}{3}\right) + j\left(\theta_2 - \frac{N}{3}\right) + j'\left(\theta_3 - \frac{N}{3}\right)\right]$$
$$= \sum_x [\varepsilon.(s_x) - 1] + j\sum_x [\varepsilon.(\sigma \times s_x) - 1] + j'\sum_x [\varepsilon.(\sigma^2 \times s_x) - 1].$$

Chaque crochet des sommes est, dans $\mathbf{R}_{(P)}$, divisible par le nombre (ou l'idéal) $\varepsilon - 1$ car

$$\varepsilon.(S_X) - 1 = \varepsilon^{X'} - 1 = (\varepsilon - 1)(\varepsilon^{X'-1} + \varepsilon^{X'-2} + \ldots + 1).$$

Cette divisibilité subsiste dans $\mathbf{R}_{(3P)}$ et s'étend à la somme $\overline{\theta}$; elle est aussi vraie pour $\overline{\theta}'$ et par suite pour la parenthèse. Puisque cette parenthèse est rationnelle, sa divisibilité par $\varepsilon - 1$ entraîne sa divisibilité par la norme de ce nombre qui est P. Le couple est donc *canonique* (§ I, n° 4).

6. *Le triplet est discriminant.* — Je fais un calcul de congruences (mod 3) dans le corps $\mathbf{R}_{(3P)}$. Je puis supprimer les coefficients multiples de 3 et remplacer par 1 les cubes de j et j'

$$\overline{\theta}^3 \equiv \sum_X [\varepsilon.(S_X)]^3, \qquad (\text{mod } 3).$$

Mais les cubes des N racines primitives sont égaux, à l'ordre près, à ces racines elles-mêmes, de sorte que

$$\overline{\theta}^3 \equiv \overline{\theta}'^3 \equiv \sum_X \varepsilon.(S_X) \equiv -1\,; \quad \begin{cases} \alpha \equiv P\alpha \equiv \alpha^2\alpha' \equiv \overline{\theta}^3 \equiv -1, \\ \alpha' \equiv P\alpha' \equiv \alpha'^2\alpha \equiv \overline{\theta}'^3 \equiv -1. \end{cases} \qquad (\text{mod } 3).$$

D'autre part la trace du triplet est égale à la somme des racines primitives, donc à -1. Les 3 sommes ou périodes construites sont donc les nombres du triplet discriminant (de trace -1) du corps unitaire (et primaire) de discriminant P^2.

7. Le raisonnement montre que le choix d'*un ordre des substitutions du groupe quotient*

$$(\sigma), \quad (\sigma^2), \quad (\sigma^3) = 1 \qquad \text{ou} \qquad (\sigma^2), \quad (\sigma^4) = (\sigma), \quad (\sigma^6) = 1;$$

détermine un ordre des nombres du triplet et, par suite, de tous les triplets du corps, à une permutation circulaire près.

Toutefois la démonstration ne précise pas la détermination de cet ordre. La recherche directe faite dans le cas du corps $\mathbf{R}_{\theta_0}$ (n° 2) pourrait être reprise dans le cas général, elle pourrait toutefois conduire à de longs calculs; il semble préférable de se borner à un calcul de congruences en utilisant des monomes en $\overline{\theta}$ et $\overline{\theta}'$ (§ II, n° 7).

Je puis déterminer l'ordre du groupe quotient par le choix d'une classe primitive g, (mod P), et de (σ) par

$$\varepsilon.(\sigma) = \varepsilon^g.$$

Cette classe g n'est ainsi définie qu'au produit près par une puissance cubique [g peut être remplacé par g^{3x+1}, ce qui substitue à (σ) une substitution $(\sigma \times s_x)$, de même classe par rapport au sous-groupe $\mathbf{G}_s$]. Je changerais l'ordre du groupe quotient en remplaçant g par g^2 (ou plus généralement par g^{3x+2}).

Ceci acquis, je choisis un nombre premier p, différent de 3 et de P, et non congru à une puissance cubique (de g) (mod P)

$$p \equiv g^{3x+\nu} \pmod{P}; \qquad [\nu \equiv 1 \text{ ou } 2, \pmod{3}].$$

Il existe de tels nombres p, d'après le théorème de la progression arithmétique, il est possible d'en démontrer aussi l'existence par un raisonnement direct (§ I, n° 2).

Il en résulte

$$\varepsilon^p = \varepsilon^{g^{x+\nu}} = \varepsilon.(\sigma^\nu \times s_x).$$

Je calcule, suivant le module p, la puissance p de θ_u; en tenant compte de la divisibilité par p des coefficients du binome

$$\theta_u^p = \left[\sum_x \varepsilon.(\sigma^u \times s_x)\right]^p \equiv \sum_x [\varepsilon.(\sigma^u \times s_x)]^p \equiv \sum_x [\varepsilon.(\sigma^{u+\nu} s_{x'})] \equiv \theta_{u+\nu}, \qquad (\text{mod } p).$$

J'en déduis la puissance p de la résolvante $\overline{\theta}$, en distinguant la classe de p, suivant le module 3

$$p \equiv +1, \pmod{3}: \qquad j^p = j, \qquad \begin{cases} \overline{\theta}^p \equiv \theta_1^p + j\theta_2^p + j'\theta_3^p, \\ \quad \equiv \overline{\theta}.(\sigma^\nu) \equiv j'^\nu \overline{\theta}, \end{cases} \qquad (\text{mod } p)$$

$$p \equiv -1, \pmod{3}: \qquad j^p = j', \qquad \begin{cases} \overline{\theta}^p \equiv \theta_1^p + j'\theta_2^p + j\theta_3^p, \\ \quad \equiv \overline{\theta}'.(\sigma^\nu) \equiv j^\nu \overline{\theta}'. \end{cases} \qquad (\text{mod } p).$$

La puissance de $\overline{\theta}'$ s'obtient en transposant j et j'.

J'utilise alors un monome simple dont la valeur est dans $\mathbf{R}_j$, il permet de calculer la classe (mod p), du monome en α, α' qui lui est égal.

$$\left.\begin{array}{ll} p \equiv +1, \pmod{3}; & \overline{\theta}^p\,\overline{\theta}' = \alpha^{\frac{2p+1}{3}} \alpha'^{\frac{p+2}{3}} \equiv j'^\nu \overline{\theta}\,\overline{\theta}' = j'^\nu \alpha\alpha'; \\ p \equiv -1, \pmod{3}; & \overline{\theta}^p\,\overline{\theta}'^{-1} = \alpha^{\frac{2p-1}{3}} \alpha'^{\frac{p-s}{3}} \equiv j^\nu\, \overline{\theta}'\,\overline{\theta}'^{-1} = j^\nu. \end{array}\right\} \quad (\text{mod } p).$$

J'en conclus (en rappelant le choix de p) :

$$p \equiv g^\nu, \pmod{P}; \quad \begin{array}{ll} p \equiv +1, \pmod{3}; & (\alpha^2\alpha')^{\frac{p-1}{3}} \equiv j'^\nu; \\ p \equiv -1, \pmod{3}; & (\alpha^2\alpha')^{\frac{p-2}{3}} \alpha \equiv j^\nu. \end{array} \quad (\text{mod } p).$$

Ces congruences (où v est 1 ou 2) permettent de déterminer celui des ordres $\|\alpha\ \alpha'\|$ ou $\|\alpha'\ \alpha\|$ du couple discriminant qui correspond au choix fait de l'ordre du groupe-quotient, par $\varepsilon.\sigma = \varepsilon^g$.

8. Je vais démontrer le cas général par récurrence sur la construction des corps, d'une part par le produit des corps abéliens déjà étudié (§ V), d'autre part par la composition des corps circulaires, dont je rappelle sommairement les propriétés.

Je considère deux corps circulaires des racines de l'unité d'indices A et B, de groupes $\mathbf{G}_S$ et $\mathbf{G}_T$. Je suppose A et B *racines carrées de discriminants de corps abéliens et premiers entre eux.*

Je désigne les racines primitives de ces corps respectivement par

$$\begin{array}{llll} \varepsilon_A.(S_X), & \text{en nombre} & \varphi(A) = M, & [(S_X) \text{ substitutions de } \mathbf{G}_S]; \\ \varepsilon_B.(T_Y), & \quad » & \varphi(B) = N, & [(T_Y) \qquad » \qquad \mathbf{G}_T]. \end{array}$$

Les groupes $\mathbf{G}_S$ et $\mathbf{G}_T$ sont abéliens, mais non nécessairement cycliques; leurs ordres M et N, en raison de l'hypothèse faite sur A et B, sont divisibles par 3.

Les produits

$$\varepsilon_A.(S_X) \times \varepsilon_B.(T_Y) \quad \text{ou} \quad \varepsilon_A \varepsilon_B.(S_X \times T_Y)$$

sont les racines primitives de l'unité, d'indice AB, en nombre

$$MN = \varphi(A) \times \varphi(B) = \varphi(AB).$$

Le groupe $\mathbf{G}_{S,T}$ de leur corps $\mathbf{R}_{(AB)}$ est le *produit direct* des groupes des corps considérés; il est formé des substitutions

$$(S_X), \quad (T_Y) \quad \text{ou} \quad (S_X T_Y);$$

définies par la loi de composition

$$\|(S_X)\quad (T_Y)\| \times \|(S_{X'})\quad (T_{Y'})\| = \|(S_X \times S_{X'})\quad (T_Y \times T_{Y'})\|.$$

Cette composition des corps et des groupes s'étend à un nombre quelconque de composants et, inversement, un corps circulaire de racines de l'unité, d'indice D, peut être obtenu en composant les corps circulaires dont les racines ont pour indices les diviseurs, premiers entre eux, de D; en l'espèce, des nombres premiers P congrus à $+1$ (mod 3) et peut être un facteur 9.

9. Je vais alors établir la propriété de récurrence :

Si deux corps abéliens, d'ordre 3, $\mathbf{R}_\xi$ et $\mathbf{R}_\eta$, *de discriminants* A^2 *et* B^2, *premiers entre eux*, et à triplets ordonnés, *sont sous-corps des corps circulaires* $\mathbf{R}_{(A)}$ et $\mathbf{R}_{(B)}$, déterminés par des groupes quotients ordonnés :

$$\begin{array}{llll} \mathbf{R}_\xi, & \text{défini par} & \mathbf{G}_S \mid \mathbf{G}_s, & \text{dans } \mathbf{R}_{(A)} \text{ (de groupe } \mathbf{G}_S); \\ \mathbf{R}_\eta, & \text{défini par} & \mathbf{G}_T \mid \mathbf{G}_t, & \text{dans } \mathbf{R}_{(B)} \text{ (de groupe } \mathbf{G}_T); \end{array}$$

le produit des corps $\mathbf{R}_\xi \mathbf{R}_\eta$ *est sous-corps de* $\mathbf{R}_{(AB)}$; son triplet discriminant est donné par les formules (5), avec une répartition par un sous-groupe $\mathbf{G}_w$ (d'index 3 de $\mathbf{G}_{S,T}$) et un ordre déterminé par celui du groupe-quotient $\mathbf{G}_{S,T} | \mathbf{G}_w$.

L'isomorphisme des groupes $\mathbf{G}_S | \mathbf{G}_s$ et $\mathbf{G}_T | \mathbf{G}_t$ étant déterminé par leur ordre, le sous-groupe $\mathbf{G}_w$, est caractérisé par son invariance pour cet isomorphisme et le sous-groupe quotient $\mathbf{G}_{S,T} | \mathbf{G}_w$ est ordonné par son isomorphisme à ces deux groupes-quotients composants.

Je suppose les sous-groupes-quotients ordonnés constitués par les classes

$$\mathbf{G}_s, \quad (\sigma)\times\mathbf{G}_s, \quad (\sigma^2)\times\mathbf{G}_s; \qquad \mathbf{G}_t, \quad (\tau)\times\mathbf{G}_t, \quad (\tau^2)\times\mathbf{G}_t.$$

Le sous-groupe $\mathbf{G}_w$, défini comme il vient d'être dit, est formé du produit direct $\mathbf{G}_s \times \mathbf{G}_t$, complété par les substitutions

$$(\sigma\times\tau^{-1})\times(\mathbf{G}_s\times\mathbf{G}_t) = (\sigma\times\tau^2)\times(\mathbf{G}_s\times\mathbf{G}_t); \qquad (\sigma^{-1}\times\tau)\times(\mathbf{G}_s\times\mathbf{G}_t) = (\sigma^2\times\tau)\times(\mathbf{G}_s\times\mathbf{G}_t).$$

Les classes du groupe-quotient $\mathbf{G}_{S,T} | \mathbf{G}_w$ peuvent être notées

$$(w_z) = (\sigma\times\tau^{-1})^u\times(s_x\times t_y); \qquad (\sigma\times w_z) = (\tau\times w_{z'}); \qquad (\sigma^2\times w_z) = (\tau^2\times w_{z'});$$

$$\left(u \text{ de } 1 \text{ à } 3;\ x \text{ de } 1 \text{ à } \frac{\mathrm{M}}{3};\ y \text{ de } 1 \text{ à } \frac{\mathrm{N}}{3};\ z \text{ ou } z' \text{ de } 1 \text{ à } \frac{\mathrm{MN}}{3}\right).$$

10. Les triplets discriminants de $\mathbf{R}_\xi$ et $\mathbf{R}_\eta$ sont; par hypothèse, définis respectivement par les sommes [u défini (mod 3)];

$$\xi_{u+1} = \sum_x [\varepsilon_{\mathrm{A}}.(\sigma^u\times s_x)], \qquad \eta_{u+1} = \sum_y [\varepsilon_{\mathrm{B}}.(\tau^u\times t_y)].$$

Je forme le produit des corps ordonnés par le choix de (σ) et (τ); son triplet discriminant a pour nombres (§ V, n° 1)

$$\vartheta_u = \xi_1\eta_{u-1} + \xi_2\eta_{u-2} + \xi_3\eta_{u-3} = \left\{\begin{array}{l} \Sigma[\varepsilon_{\mathrm{A}}.(s_x)][\varepsilon_{\mathrm{B}}.(\tau^{u+1}\times t_y)] \\ + \Sigma[\varepsilon_{\mathrm{A}}.(\sigma\times s_x)][\varepsilon_{\mathrm{B}}.(\tau^u\times t_y)] \\ + \Sigma[\varepsilon_{\mathrm{A}}.(\sigma^2\times s_x)][\varepsilon_{\mathrm{B}}.(\tau^{u-1}\times t_y)]. \end{array}\right.$$

Les nombres des 3 sommes sont déduits de la racine primitive $\varepsilon_A\varepsilon_B$ par les substitutions

$$\begin{aligned}&[(\tau^{u+1}\times s_x\times t_y), \quad (\tau^u\times\sigma\times s_x\times t_y), \quad (\tau^{u-1}\times\sigma^2 s_x t_y)] \\ &\quad = (\tau^{u+1})\times[(s_x\times t_y), \quad (\sigma\times\tau^{-1}\times s_x\times t_y), \quad (\sigma^2\times\tau\times s_x\times t_y)] = (\tau^{u+1}\times w_z);\end{aligned}$$

qui sont celles de la classe d'indice $u+2$ du groupe-quotient $\mathbf{G}_{S,T} | \mathbf{G}_w$. La somme qui constitue ϑ_u est donc l'une des sommes données par les formules (9) dans le corps circulaire $\mathbf{R}_{(AB)}$; de façon précise

$$\vartheta_u = \theta_{u+2}; \qquad (u \text{ défini mod } 3).$$

11. J'ai ainsi démontré la propriété de récurrence; il est visible qu'un changement d'ordre dans un seul des sous-groupes-quotients change le corps produit, tandis qu'un changement d'ordre simultané dans les deux composants ne change que l'ordre des triplets du produit.

Cette propriété de récurrence appliquée de proche en proche montre qu'un produit d'un nombre quelconque de corps abéliens primaires dont les discriminants sont différents et ont pour produit D^2 peut être construit en répartissant les racines primitives de l'unité, d'indice D, suivant les classes d'un groupe-quotient convenable d'ordre 3, et réciproquement.

Le corps des racines de l'unité, d'indice D, a ainsi 2^{h-1} *sous-corps abéliens,* d'ordre 3, h étant le nombre des facteurs premiers de D.

12. Les corps quadratiques sont aussi sous-corps de corps circulaires; ceci est précisé par l'énoncé suivant (dont la vérification est plus immédiate que dans le cas des corps du troisième ordre) :

Un corps quadratique de discriminant D (constitué comme il est dit § V, n° 5) *est sous-corps du corps circulaire* $\mathbf{R}_{|D|}$ *des racines d'indice* $|D|$ *de l'unité* [de degré $\varphi(|D|)$].

Son couple discriminant (§ IV, n° 8) est constitué par deux sommes de racines primitives réparties par un groupe quotient $\mathbf{G}_S|\mathbf{G}_s$ d'ordre 2, du groupe de Galois $\mathbf{G}_S$ de $\mathbf{R}_D$

$$\theta_1 = \sum_x \varepsilon_D.(s_x); \qquad \theta_2 = \sum_x \varepsilon_D.(\sigma \times s_x).$$

(mêmes notations qu'au n° 1 du paragraphe VII; $\sigma^2 = 1$).

Les trois corps simples non unitaires signalés au paragraphe IV, n° 8, sont définis par

$$(a) \qquad \theta_1 = \varepsilon, \qquad \theta_2 = \varepsilon^3;$$

$\varepsilon = i$, racine primitive quatrième de l'unité;

$$(b) \qquad \theta_1 = \varepsilon + \varepsilon^3 = i\sqrt{2}, \qquad \theta_2 = \varepsilon^5 + \varepsilon^7 = -i\sqrt{2};$$

$$(c) \qquad \theta_1 = \varepsilon + \varepsilon^7 = \sqrt{2}, \qquad \theta_2 = \varepsilon^3 + \varepsilon^5 = -\sqrt{2};$$

$\varepsilon = \frac{1+i}{\sqrt{2}}$, racine primitive huitième de l'unité, ou zéro du polynome irréductible : $x^4 + 1$.

Contrairement à ce qui se passe pour le troisième degré, la composition de deux corps quadratiques ne peut être faite que d'une façon (§ V, n° 7) et ne donne qu'un seul corps nouveau. Toutefois comme le corps circulaire des racines huitièmes a deux sous-corps quadratiques, il en résulte que :

Tout corps circulaire, de racines d'indice $|D|$ *de l'unité, a un et un seul sous-corps quadratique si D est impair ou multiple de 4 seulement; il a deux sous-corps si D est multiple de* 8.

VIII. — Loi de réciprocité.

1. La construction d'un corps abélien comme sous-corps d'un corps circulaire permet de démontrer assez aisément la *loi de réciprocité* (entre la racine carrée D du discriminant et un nombre premier p décomposé dans le corps) annoncée ci-dessus (§ VI, n° 8). Elle peut être énoncée comme suit :

La qualité d'un nombre premier p, d'être un idéal premier, ou un produit d'idéaux premiers (distincts), **dans un corps abélien,** d'ordre 3, **de discriminant** D^2, **est la même pour tous les nombres premiers d'une classe** (mod D) (ou appartenant à une progression arithmétique de raison D).

Il n'y a pas lieu d'ajouter la qualité d'être puissance d'idéal premier. Elle exige en effet que p soit diviseur de D et, dans ce cas, il n'y a pas d'autre nombre premier congru à p (mod D).

2. La racine carrée D d'un discriminant est un produit de facteurs premiers P_r, congrus à $+1$, (mod 3), et éventuellement d'un facteur 9. Je considère le corps circulaire $\mathbf{R}_{(D)}$ des racines de l'unité, dont l'indice est un tel nombre D. Son degré est

$$\varphi(D) = N = M_1 M_2 \ldots M_h; \qquad (M_r = P_r - 1; \quad M_1 = 6, \text{ si } P_1 = 9).$$

Son groupe $\mathbf{G}_S$ (de Galois) est isomorphe au groupe des classes (mod D) premières avec D. Il y a donc aussi isomorphisme des sous-groupes et des groupes-quotients, en particulier de $\mathbf{G}_S \mid \mathbf{G}_s$ ($\mathbf{G}_s$ d'index 3) qui sert à construire les sommes (ou périodes) qui définissent un corps abélien (§ VII, n° 1). Je précise la construction du groupe des classes et d'un tel sous-groupe quotient, qu'il n'y a pas d'ambiguïté à désigner par les mêmes notations $\mathbf{G}_S$ et $\mathbf{G}_S \mid \mathbf{G}_s$.

Si D est égal à un nombre premier P, il suffit de choisir une racine primitive g (mod P) [il y en a $\varphi(P-1)$]; les groupes sont respectivement définis par

$$\mathbf{G}_S: \ g^X, \quad \mathbf{G}_s: \ g^{3x} \quad (\text{mod } P); \qquad \left[X, \text{ mod } N; \quad x, \text{ mod } \frac{N}{3}\right];$$

$$\mathbf{G}_S \mid \mathbf{G}_s: \ g\mathbf{G}_s, \ g^2\mathbf{G}_s, \ \mathbf{G}_s, \qquad (\text{ou } g^2\mathbf{G}_s, \ g\mathbf{G}_s, \ \mathbf{G}_s).$$

Cette constitution est encore valable pour $D = 9$, je puis alors prendre pour g l'une des classes ± 2.

Dans le cas d'un discriminant D composé, je considère le corps comme un produit de corps primaires, de discriminants P_r^2, chacun ordonné, comme il vient d'être dit, par le choix d'une classe primitive g'_r (mod P_r). Je détermine alors des classes g_r (mod D), par les congruences

$$g_r \equiv g'_r, \quad (\text{mod } P_r); \qquad g_r \equiv +1, \quad \left(\text{mod } \frac{D}{P_r}\right).$$

Le groupe des classes (mod D), isomorphe à $\mathbf{G}_S$ est constitué par les monomes

$$g_1^{X_1} g_2^{X_2} \ldots g_h^{X_h}, \quad (\text{mod } D); \qquad [X_r \text{ défini mod } P_r].$$

Le sous-groupe $\mathbf{G}_s$, d'index 3, dont j'ai indiqué la formation de proche en proche, est formé des classes

$$z \equiv g_1^{3x_1} g_2^{3x_2} \ldots g_h^{3x_h} (g_1 g_2^{-1})^{u_2} (g_1 g_3^{-1})^{u_3} \ldots (g_1 g_h^{-1})^{u_h} \qquad (\text{mod } D)$$

$\left(x_r \text{ défini mod } \frac{P_r}{3};\ u_r \text{ défini mod } 3\right)$.

Le nombre des termes est

$$\frac{P_1}{3} \frac{P_2}{3} \ldots \frac{P_h}{3} 3^{h-1} = \frac{P_1 P_2 \ldots P_h}{3} = \frac{D}{3}.$$

Les classes du groupe-quotient peuvent être définies indifféremment par les représentants

$$g_r, \quad g_r^2, \quad g_r^3 \quad (\text{quel que soit } r);$$

ce qui montre l'isomorphisme de ce groupe avec chacun des groupes-quotients des corps constituants, isomorphes entre eux.

Je précise la construction des substitutions (S) elles-mêmes; je désigne par ε_1, ε_2, ..., ε_h des racines primitives de l'unité d'indices respectifs P_1, P_2, ..., P_h. La substitution (S_z), correspondant à une classe z (mod D), peut être exprimée par une puissance d'une racine primitive d'indice D (produit des racines précédentes)

$$[\varepsilon_1 \varepsilon_2 \ldots \varepsilon_h].(S_z) = [\varepsilon_1 \varepsilon_2 \ldots \varepsilon_h]^z.$$

L'exponentiation peut être répartie sur chaque racine du monome, tenant compte des facteurs de l'exposant qui sont congrus à $+1$, suivant les divers facteurs de D

$$\varepsilon_1^{z_1} \varepsilon_2^{z_2} \ldots \varepsilon_h^{z_h} \left\{ \begin{array}{ll} z_r \equiv g_r^{3x_r + 2u_r} & (\text{mod } P_r); \\ z_1 \equiv g_1^{3x_1 + (u_2 + \ldots + u_h)} & (\text{mod } P_1). \end{array} \right.$$

3. La relation entre la qualité de décomposition d'un nombre premier p, dans le corps $\mathbf{R}_0$ et la classe à laquelle il appartient (mod D) peut alors être énoncée comme suit :

Pour que, dans le corps $\mathbf{R}_0$, construit dans le corps $\mathbf{R}_{(D)}$ avec une répartition par un groupe quotient $\mathbf{G}_S \mid \mathbf{G}_s$, *un nombre premier p soit décomposable, il faut et il suffit que p soit dans une classe du groupe* $\mathbf{G}_s$ *des classes (mod D).*

La démonstration de cette propriété peut être faite en appliquant la condition de décomposition d'un nombre premier dans un corps circulaire $\mathbf{R}_{(D)}$; il me semble intéressant de donner un raisonnement direct.

Je suppose que p, non diviseur de D, admet un facteur idéal premier $\mathfrak{P}$, du premier degré et par suite de norme p. Un nombre θ_1 du triplet discriminant est congru (mod $\mathfrak{P}$) à un nombre rationnel c et l'un au moins des deux autres conjugués $\theta_2 - c$, $\theta_3 - c$ n'est pas dans $\mathfrak{P}$. Il en résulte, d'après la divisibilité des coefficients du binome et le théorème de Fermat

$$(\theta_1 - c)^p \equiv \theta_1^p - c, \quad (\text{mod } p); \qquad \text{et} \qquad \left\{ \begin{array}{c} \theta_1^p - \theta_1 \equiv 0, \\ \theta_1^p - \theta_2 \quad \text{ou} \quad \theta_1^p - \theta_3 \not\equiv 0, \end{array} \right. \qquad (\text{mod } \mathfrak{P}).$$

L'expression de θ_1 dans $\mathbf{R}_D$ donne d'autre part les congruences

$$\theta_1^p = \left[\sum_x \varepsilon_D.(s_x) \right]^p \equiv \sum_x [\varepsilon_D.(s_x)]^p \equiv \sum_x [\varepsilon_D.(\sigma_u \times s_x)] \equiv \theta_{1+u}, \qquad (\text{mod } p);$$

si le nombre p appartient à une classe $g^u \mathbf{G}_s$ [u défini (mod 3)]. Il en résulte

$$\theta_1 \equiv \theta_1^p \equiv \theta_1^{p^2} \equiv \theta_{1+u} \equiv \theta_{1+2u}, \qquad (\text{mod } p).$$

D'après la propriété précédente, ceci exige que u soit congru à zéro (mod 3), c'est-à-dire que p appartienne au groupe $\mathbf{G}_s$.

Réciproquement, s'il en est ainsi, la congruence qui en résulte

$$0 \equiv \theta_1^p - \theta_1 \equiv (\theta_1 - 1)(\theta_1 - 2) \ldots (\theta_1 - p) \qquad (\text{mod } p)$$

entraîne l'existence d'un facteur (idéal) commun à p et à l'un des facteurs $(\theta_1 - c)$, c'est-à-dire encore l'existence d'un idéal

$$\mathfrak{P} = (p, \theta_1 - c),$$

diviseur proprement dit de p, ce qui, d'après le raisonnement déjà fait (§ VI, n° 6) entraîne la décomposition de p.

4. *Exemples.* — *a*. J'ai déjà dit que le corps $\mathbf{R}_{0_0}$ est engendré par des sommes (ou périodes) dans le corps $\mathbf{R}_{(9)}$, de degré 6. Suivant le module 9, je puis prendre $+2$ comme classe primitive et les classes de $\mathbf{G}_s$ définies par ce choix sont

$$2^3 \text{ et } 2^6, \quad \text{ou} \quad -1 \text{ et } +1, \quad (\text{mod } 9).$$

Dans le groupe-quotient l'ordre des classes défini par les puissances de 2 est

$$(-1, +1), \quad (-2, +2), \quad (-4, +4), \quad (\text{mod } 9);$$

c'est celui qui a été adopté au paragraphe VII, n° 2; il lui correspond le couple discriminant ordonné $\| 3j \quad 3j' \|$ d'après le calcul fait.

Les nombres premiers, décomposables dans $\mathbf{R}_{0_0}$ sont ceux qui sont congrus à ± 1, (mod 9), en plus du facteur 3 du discriminant. Les premiers sont 17, 19, 37, 53, 71, 73, 89, ..., ce sont les *modules* pour lesquels le polynome fondamental (du triplet discriminant)

$$f(x) = x^3 - 3x + 1$$

a des racines.

b. Le corps unitaire primaire, de discriminant 7^2, est engendré par des périodes dans le corps $\mathbf{R}_{(7)}$, de degré 6. Suivant le module 7, je puis prendre $+3$ comme classe primitive et les classes de $\mathbf{G}_s$ (encore au nombre de 2), définies par ce choix, sont

$$3^3 \text{ et } 3^6, \quad \text{ou} \quad -1 \text{ et } +1, \quad (\text{mod } 7).$$

Dans le groupe quotient, l'ordre des classes, défini par les puissances de 3 est

$$(-1, +1), \quad (-3, +3), \quad (-3^2, +3^2) \equiv (-2, +2) \qquad (\text{mod } 7).$$

D'autre part la décomposition de 7 dans $\mathbf{R}_j$, en facteurs d'un couple unitaire positif est

$$7 = (-j + 2j')\,(-j' + 2j).$$

J'applique la méthode du paragraphe VII, n° 7 pour déterminer l'ordre du couple qui correspond à celui du groupe-quotient (ou des triplets du corps); je prends pour exposant p

$$p = 2 \equiv 3^2 \quad (\text{mod } 7), \qquad \left[\frac{p-2}{3} = 0; \qquad \nu \equiv 2 \quad (\text{mod } 3)\right].$$

La congruence, qui devient

$$\alpha \equiv j^2 = j' \qquad (\text{mod } 2);$$

est vérifiée pour $\alpha = -j' + 2j$ de sorte que le couple cherché est

$$\| -j' + 2j \quad -j + 2j' \|;$$

le polynome fondamental, déjà indiqué (§ IV, n° 5) est

$$f(x) = x^3 - x^2 - 2x + 1.$$

Les nombres premiers décomposables dans le corps sont (en plus de 7) ceux qui sont congrus à ± 1 (mod 7); les premiers sont 13, 29, 41, 43, 71, 83, 97, ... ce sont les modules suivant lesquels le polynome fondamental a des racines.

c. Je forme le produit des deux corps précédents, ordonnés comme il a été convenu; le couple discriminant de ce produit est

$$\| -j' + 2j \quad -j + 2j' \| \times \| 3j \quad 3j' \| = \| 3j + 9j' \quad 3j' + 9j \|;$$

le polynome fondamental du triplet discriminant est (calcul général des § II, n° 4 et § IV, n^{os} 6 et 7)

$$f(x) = x^3 - 3 \times 7x + 28.$$

Ce produit peut être engendré par des périodes dans le corps circulaire $\mathbf{R}_{(63)}$, de degré $6 \times 6 = 36$. Je puis exprimer son groupe en classes (mod 63) au moyen de générateurs construits comme il a été dit au n° 2 précédent

$$-29 \begin{cases} \equiv +2 & (\text{mod } 9); \\ \equiv +1 & (\text{mod } 7); \end{cases} \qquad +10 \begin{cases} \equiv +1 & (\text{mod } 9); \\ \equiv +3 & (\text{mod } 7); \end{cases}$$

son expression est

$$\mathbf{G}_S : (+29)^{X_1} \times (+10)^{X_2} \quad (\text{mod } 63), \qquad (X_1 \text{ et } X_2 \text{ définis mod } 6).$$

Le sous-groupe $\mathbf{G}_s$, défini par l'isomorphisme des sous-groupes considérés dans les corps composants est

$$(+29)^{3x_1} \times (+10)^{3x_2} \times (29.10^{-1})^{u_2}, \quad (\text{mod } 63); \qquad [x_1, x_2 \quad \text{mod } 2; \qquad u_2 \quad \text{mod } 3];$$

ou

$$\pm 1, \quad \pm 8, \quad \pm 2, \quad \pm 16, \quad \pm 4, \quad \pm 32, \qquad (\text{mod } 63).$$

Les nombres premiers décomposables dans ce corps sont, en plus de 3 et 7, ceux qui sont dans ces classes; les premiers sont

2, 31, 47, 59, 61, 67, 71, 79, 127, 157, 173, 181, 191, 193, 197, ...

ils pourraient être retrouvés par la recherche des facteurs premiers des valeurs (pour x entier) du polynome fondamental, ce qui donnerait lieu à un calcul analogue à celui du crible d'Ératosthène.

J'obtiens un corps différent en changeant l'ordre de l'un des groupes quotients, par exemple de $\mathbf{R}_j$, le couple discriminant du nouveau corps est

$$\| -j' + 2j \quad -j + 2j' \| \, \| 3j' \quad 3j \| = \| -9j - 6j' \quad -9j - 6j \|;$$

et son polynome fondamental est

$$f(x) = x^3 - 3 \times 7x - 35.$$

Le sous-groupe $\mathbf{G}_s$ est

$$(+29)^{3x_1} \times (+10)^{3x_2} \times (29^2.10^{-1})^{u_2}, \quad (\text{mod } 63); \qquad [x_1, x_2 \quad \text{mod } 2; \qquad u_2 \quad \text{mod } 3]$$

ou

$$\pm 1, \quad \pm 8, \quad \pm 25, \quad \pm 11, \quad \pm 5, \quad \pm 23, \qquad (\text{mod } 63).$$

Les nombres premiers décomposables dans ce corps sont, en plus des facteurs 3 et 7 du discriminant, ceux qui appartiennent à ces classes, dont les deux premières sont communes avec le corps précédent. Les premiers de ces nombres sont

5, 11, 23, 71, 101, 103, 127, 131, 137, 149, 151, 181, 197, ...

5. La loi célèbre de *réciprocité quadratique*, énoncée avec le symbole de Legendre est

$$\left(\frac{p}{d}\right)\left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\frac{d-1}{2}}.$$

Si p est premier, le symbole $\left(\frac{d}{p}\right)$ est égal à -1 ou à $+1$ suivant l'impossibilité ou la possibilité de la congruence

$$x^2 - d \equiv 0 \pmod{p}.$$

La possibilité de cette congruence est liée elle-même (ainsi qu'il a été rappelé § VI, n° 10) à la décomposition du nombre premier p en idéaux, dans le corps quadratique engendré par $\sqrt{d}$. On en conclut aisément en considérant le discriminant D du corps, au lieu du nombre d, et en utilisant le caractère quadratique du nombre 2, une conséquence de la loi analogue à l'énoncé ci-dessus :

La qualité d'un nombre premier p, d'être un idéal premier, ou un produit de deux idéaux premiers (distincts) *dans un corps quadratique, de discriminant D, est la même pour les nombres premiers d'une classe* (mod $|D|$) (ou appartenant à une progression arithmétique de raison $|D|$).

On sait que la loi de réciprocité a fait l'objet d'un grand nombre de démonstrations *directes* ou élémentaires, mais qui lui laissent cependant un caractère assez mystérieux. Il est possible d'en donner une démonstration, en considérant comme il a été fait pour les corps du troisième degré, la double génération d'un corps quadratique, par l'introduction d'une racine d'un nombre entier, ou comme sous-corps d'un corps circulaire. Cette méthode également connue permet de prouver non seulement la conséquence de la loi, mais la loi elle-même sous la forme rappelée, y compris le caractère quadratique des nombres 2 et -1. Il me semble qu'elle en constitue une preuve plus directe (ou plus naturelle).