

8.

Applications de l'Algèbre à l'Arithmétique transcendante.

(Par Mr. G. Eisenstein à Berlin.)

Etant proposé deux équations algébriques quelconques, on pourra en éliminer la quantité inconnue x de deux manières différentes, soit en mettant dans la seconde à la place de x sa valeur tirée de la première, soit en mettant dans la première à la place de x sa valeur tirée de la seconde, sans changer essentiellement le résultat de l'élimination. Nous ferons voir dans ce qui suit que les lois de réciprocité pour les résidus quadratiques, cubiques et biquadratiques, (théorèmes si célèbres tant par la difficulté de leur démonstration, que par l'assiduité avec laquelle les plus grands géomètres s'en sont occupés) ne sont autre chose que l'interprétation arithmétique du simple fait algébrique dont nous venons de parler. Ainsi par exemple, en posant $\sin v = x$, si l'on désigne par p et q deux nombres premiers impairs (réel) et par $x = \pm \alpha$, $x = \pm \beta$ resp. les ensembles des racines des deux équations $\frac{\sin p v}{\sin v} = 0$, $\frac{\sin q v}{\sin v} = 0$, nous verrons que les résidus de $p^{\frac{1}{2}(q-1)}$ et $q^{\frac{1}{2}(p-1)}$ suivant les modules q , p dépendent resp. des deux expressions $\Pi(\beta^2 - \alpha^2)$ et $\Pi(\alpha^2 - \beta^2)$, où la multiplication se rapporte à toutes les valeurs de α et de β ; il existe des résultats analogues pour les résidus cubiques et biquadratiques. La méthode qui nous conduira à ces résultats est très simple, elle traite d'une manière parfaitement symétrique les deux nombres à comparer, et conserve dans les démonstrations l'analogie qui existe entre les théorèmes qui se rapportent aux résidus des différentes puissances. Au reste on peut considérer ce que nous allons exposer comme les premiers éléments d'une nouvelle doctrine où l'on renvoie les questions arithmétiques à l'algèbre et à l'analyse, de manière qu'alors toutes les difficultés se réduisent à celles qu'offre le calcul. J'entre en matière en commençant par les résidus quadratiques.

§. 1.

Résidus quadratiques.

Etant donné un nombre premier impair (réel et positif) p , on peut toujours concevoir un système de résidus pour le module p *) distribué en deux groupes tels, que les termes qui composent le deuxième groupe sont opposés à ceux du premier; nous représenterons les termes généraux de ces deux groupes par r et par $-r$; on pourra p. e. prendre pour r les nombres $1, 2, 3, \dots, \frac{1}{2}(p-1)$ et pour $-r$ les nombres $-1, -2, -3, \dots, -\frac{1}{2}(p-1)$. Cela posé, si l'on multiplie tous les r par un entier quelconque q non divisible par p , les résidus des produits qr se trouveront en partie parmi les r et en parti parmi les $-r$. En posant, selon ces deux cas que nous venons de distinguer,

$$\text{ou } qr \equiv r' \text{ ou } qr \equiv -r' \pmod{p},$$

de sorte que r' se trouve toujours parmi les r , on aura respectivement:

$$\sin \frac{qr\omega}{p} = \sin \frac{r'\omega}{p}, \quad \text{ou } \sin \frac{qr\omega}{p} = -\sin \frac{r'\omega}{p},$$

où l'on a fait pour abrégér $\omega = 2\pi$. On aura donc dans tous les cas

$$qr \equiv r' \cdot \frac{\sin \frac{qr\omega}{p}}{\sin \frac{r'\omega}{p}} \pmod{p}.$$

Substituant dans cette expression de r toutes ses $\frac{1}{2}(p-1)$ valeurs et multipliant entre elles toutes les expressions que cela donne, on obtiendra, en observant encore que tous les r' coïncident avec tous les r :

$$q^{k(p-1)} \prod r \equiv \prod r' \cdot \frac{\prod \sin \frac{qr\omega}{p}}{\prod \sin \frac{r'\omega}{p}} \equiv \prod r \cdot \prod \left\{ \frac{\sin \frac{qr\omega}{p}}{\sin \frac{r\omega}{p}} \right\} \pmod{p},$$

donc, si l'on divise les deux membres de cette congruence par $\prod r$, ce qui est permis, $\prod r$ n'étant pas divisible par le module p , on aura

$$(1.) \quad q^{k(p-1)} \equiv \prod \left\{ \frac{\sin \frac{qr\omega}{p}}{\sin \frac{r\omega}{p}} \right\} \pmod{p}.$$

Cette formule exprime le caractere quadratique de q par rapport à p . Supposant maintenant que q soit aussi un nombre premier impair, le caractère quadratique de p par rapport à q sera exprimé d'une manière analogue par la formule

*) à l'exclusion de celui des termes d'un tel système qui est un multiple du module; ce qu'on suppose toujours tacitement.

$$(2.) \quad p^{\frac{1}{2}(q-1)} \equiv \Pi \left\{ \frac{\sin \frac{p q \omega}{q}}{\sin \frac{q \omega}{q}} \right\} \pmod{q},$$

(la multiplication se rapportant à q) qui est l'expression générale d'une suite de nombres qui joints aux $-q$ composent un système de résidus pour le module q .

Il ne s'agit donc que de comparer entre eux les deux caractères quadratiques à droite dans les formules (1.) et (2.). Si l'on fait $\sin v = x$, les quantités

$$\frac{\sin p v}{\sin v} = P, \quad \frac{\sin q v}{\sin v} = Q$$

seront des fonctions entières de x resp. des degrés $p-1$ et $q-1$; de plus, en posant $\sin \frac{q \omega}{q} = \alpha$, $\sin \frac{p \omega}{p} = \beta$, les racines de l'équation $P = 0$ seront désignées par $\pm \alpha$ et celles de l'équation $Q = 0$ par $\pm \beta$. Cela étant, le deuxième membre de la formule (1.) sera équivalent au produit des valeurs que prend l'expression Q en y mettant pour x toutes les valeurs de α , et de même on obtiendra le deuxième membre de la formule (2.) en mettant dans P pour x toutes les valeurs de β , et faisant le produit des expressions qui en résultent. Or on a

$$P = \frac{(-1)^{\frac{1}{2}(p-1)}}{2^{p-1}} \Pi(x^2 - \alpha^2), \quad Q = \frac{(-1)^{\frac{1}{2}(q-1)}}{2^{q-1}} \Pi(x^2 - \beta^2),$$

donc il viendra

$$(3.) \quad q^{\frac{1}{2}(p-1)} \equiv C \Pi(\alpha^2 - \beta^2) \pmod{p},$$

$$(4.) \quad p^{\frac{1}{2}(q-1)} \equiv C \Pi(\beta^2 - \alpha^2) \pmod{q},$$

où chaque valeur de α doit être combinée avec chaque valeur de β . C est une constante qui se trouve être $C = \frac{(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}}{2^{\frac{1}{2}(p-1)(q-1)}}$. Maintenant le nombre

des α est $= \frac{1}{2}(p-1)$, et le nombre des β est $= \frac{1}{2}(q-1)$, par conséquent le nombre des combinaisons α et β sera $= \frac{1}{2}(p-1)\frac{1}{2}(q-1)$, d'où enfin on tire

$$\Pi(\alpha^2 - \beta^2) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} \Pi(\beta^2 - \alpha^2).$$

Cette dernière équation comparée avec (3.) et (4.) donne immédiatement la loi de reciprocité pour les résidus quadratiques. Si l'on veut éviter la constante C , il faut se servir des tangentes au lieu des sinus.

§. 2.

Résidus biquadratiques.

Les résidus biquadratiques peuvent être traités d'une manière absolument semblable. Les fonctions elliptiques, ou plutôt cette espèce particulière de

fonctions elliptiques qui se rapportent à la lemniscate, jouent ici le rôle des sinus; il faut donc dire d'abord quelques mots sur ces fonctions.

Nous désignerons par $x = \sin \operatorname{am} v$ la fonction de v qui satisfait à l'équation différentielle

$$dx = dv \cdot \sqrt{1-x^4},$$

et qui en même temps s'évanouit avec v . Cette fonction est périodique de deux manières; en effet en posant $\omega = 4 \int_0^1 \frac{dx}{\sqrt{1-x^4}}$, on a $\sin \operatorname{am}(v+k\omega) = \sin \operatorname{am} v$,

k étant un entier complexe quelconque de la forme $a+bi$, où a et b sont des entiers réels. Une autre propriété de cette fonction est exprimée par

$$\sin \operatorname{am} iv = i \sin \operatorname{am} v,$$

propriété très-importante pour notre recherche et qui se déduit immédiatement de l'équation différentielle, en observant que celle-ci ne varie pas par le changement simultané de x en ix et de v en iv . On sait en outre par les recherches d'Abel et de Mr. Jacobi *) que $\sin \operatorname{am}(u+v)$ peut être exprimé algébriquement par $\sin \operatorname{am} u$ et $\sin \operatorname{am} v$, et surtout, qu'en prenant pour m un entier complexe impair, on peut réduire $\sin \operatorname{am} mv$ à une fonction rationnelle de $\sin \operatorname{am} v$.

Soit $m = a+bi$ un nombre premier complexe impair; soit la norme de m , c'est à dire l'entier réel et positif $a^2 + b^2 = p = N(m)$; on pourra toujours partager un système de résidus pour le module m , qui contient $p-1$ termes à l'exclusion de celui qui est divisible par le module, en quatre groupes, de manière que les termes du 2^{ième}, 3^{ième} et 4^{ième} groupe se déduisent de ceux du premier en multipliant ceux de celui-ci par i , par -1 , et par $-i$ respectivement. Nous désignerons indéfiniment les termes de ces quatre groupes par $r, ir, -r, -ir$ resp. Multipliant alors tous les r par un entier complexe quelconque n non divisible par m , les résidus des produits nr se trouveront en partie parmi les r , en partie parmi les $ir, -r$, ou $-ir$. Soit selon ces quatre cas qu'il y a à distinguer,

$$nr \equiv r', ir', -r', -ir', \pmod{m},$$

où r' se trouve parmi les r . Cela posé, on aura selon les quatre cas

$$\frac{\sin \operatorname{am} \frac{nr\omega}{m}}{\sin \operatorname{am} \frac{r'\omega}{m}} = 1, i, -1, \text{ ou } -i;$$

*) Voir p. e. le 2^d, 3^{ième} et 4^{ième} volume de ce journal. Il paraît que Mr. Gauss était déjà à la fin du dernier siècle en possession des principaux théorèmes sur ces fonctions; en effet dans ses disq. arithm. il a promis un ouvrage étendu sur ces fonctions, mais il paraît que les circonstances et d'autres travaux l'ont empêché d'exécuter son projet.

on aura donc dans tous les cas

$$nr \equiv r' \frac{\sin \operatorname{am} \frac{nr\omega}{m}}{\sin \operatorname{am} \frac{r'\omega}{m}} \pmod{m},$$

d'où, en observant que tous les r' coïncident avec tous les r , et que Πr n'est point divisible par m , on tire

$$(1.) \quad n^{\frac{1}{2}(p-1)} \equiv \Pi \left\{ \frac{\sin \operatorname{am} \frac{nr\omega}{m}}{\sin \operatorname{am} \frac{r\omega}{m}} \right\} \pmod{m},$$

le signe Π s'étendant à tous les r . Supposant que n , ainsi que m , soit un nombre premier complexe impair et que le système de résidus pour le module n soit aussi distribué en quatre groupes tels que leurs termes généraux sont représentés par $\varrho, i\varrho, -\varrho, -i\varrho$, on aura d'une manière analogue

$$(2.) \quad m^{\frac{1}{2}(q-1)} \equiv \Pi \left\{ \frac{\sin \operatorname{am} \frac{m\varrho\omega}{n}}{\sin \operatorname{am} \frac{\varrho\omega}{n}} \right\} \pmod{n},$$

q étant la norme de n et la multiplication se rapportant à toutes les valeurs de ϱ .

Nous avons déjà remarqué qu'on peut exprimer $\sin \operatorname{am} m v$ et par conséquent aussi $\frac{\sin \operatorname{am} m v}{\sin \operatorname{am} v}$ par une fonction rationnelle de $\sin \operatorname{am} v$. Il existe entre le numérateur et le dénominateur de cette fonction rationnelle, qui sont du degré $p-1$, une relation remarquable qui dépend du résidu de m par rapport au module $2+2i$. Cette relation se réduit à sa plus simple forme si l'on suppose m *primaire*, c'est à dire $\equiv 1 \pmod{2+2i}$; dans ce cas la valeur de $\frac{\sin \operatorname{am} m v}{\sin \operatorname{am} v}$ prend la forme $\frac{\varphi(x)}{x^{p-1}\varphi\left(\frac{1}{x}\right)}$, x étant $= \sin \operatorname{am} v$ et $\varphi(x)$ une

fonction entière de x du degré $p-1$. En effet, supposant la fraction $\frac{\varphi(x)}{\psi(x)}$ réduite à sa plus simple expression et le coefficient de la plus haute puissance dans le numérateur égal à l'unité, ce qui est permis, si l'on fait

$$\frac{\sin \operatorname{am} m v}{\sin \operatorname{am} v} = \frac{\varphi(x)}{\psi(x)},$$

l'expression $y = x \frac{\varphi(x)}{\psi(x)}$ qui s'évanouit avec x , satisfera à l'équation différentielle $\frac{dy}{\sqrt{(1-y^4)}} = \frac{m dx}{\sqrt{(1-x^4)}}$, d'où l'on voit que tous les exposants des différentes puissances dans $\varphi(x)$ et dans $\psi(x)$ sont des multiples de quatre; posant

$y = \frac{1}{\eta}$, $x = \frac{1}{i^\mu \xi}$, où μ désigne un entier indéterminé, l'équation différentielle que nous venons d'écrire se changera par cette substitution en $\frac{i^\mu d\eta}{\sqrt{(\eta^4 - 1)}} = \frac{m d\xi}{\sqrt{(1 - \xi^4)}}$.

Cette dernière équation sera donc satisfaite par l'intégrale $\eta = i^\mu \xi \frac{\psi\left(\frac{1}{\xi}\right)}{\varphi\left(\frac{1}{\xi}\right)}$, et

comme il est facile de voir que celle-ci, réduite à la forme $i^\nu \xi \frac{\xi^{p-1} \psi\left(\frac{1}{\xi}\right)}{\xi^{p-1} \varphi\left(\frac{1}{\xi}\right)}$,

doit coïncider avec l'intégrale y qui satisfait à la même équation différentielle, on pourra, à une unité complexe près, évaluer entre eux séparément les numérateurs et les dénominateurs des deux intégrales dont il s'agit. Cela donne

$\psi(x) = i^\nu x^{p-1} \varphi\left(\frac{1}{x}\right)$, ν étant un entier réel. Pour en déterminer la valeur,

il suffira de donner à v une valeur particulière. Posant p. e. $v = \frac{1}{4}\omega$, on

trouvera $x = \sin \operatorname{am} \frac{1}{4}\omega = 1$ et $\sin \operatorname{am} \frac{1}{4}(m\omega) = \frac{\varphi(1)}{i^\nu \varphi(1)} = i^{-\nu}$; or pour une

valeur primaire de m on a $\sin \operatorname{am} \frac{1}{4}(m\omega) = +1$ (Tome II. Page 111 de ce journal)

et par suite $i^\nu = 1$, donc on a définitivement $\frac{\sin \operatorname{am} m v}{\sin \operatorname{am} v} = \frac{\varphi(x)}{x^{p-1} \varphi\left(\frac{1}{x}\right)}$, pour une

valeur *primaire* de m ; ce qu'il s'agissait de prouver.

Si donc on suppose que m et n tous les deux soient $\equiv 1 \pmod{2 + 2i}$, et qu'on fasse

$$\frac{\sin \operatorname{am} m v}{\sin \operatorname{am} v} = \frac{\varphi(x)}{x^{p-1} \varphi\left(\frac{1}{x}\right)}, \quad \frac{\sin \operatorname{am} n v}{\sin \operatorname{am} v} = \frac{f(x)}{x^{q-1} f\left(\frac{1}{x}\right)},$$

$$\sin \operatorname{am} \frac{r\omega}{m} = \alpha, \quad \sin \operatorname{am} \frac{\rho\omega}{n} = \beta,$$

les racines de l'équation $\varphi(x) = 0$ seront données par $\pm\alpha$, $\pm i\alpha$, et celles de l'équation $f(x) = 0$ par $\pm\beta$, $\pm i\beta$, de sorte qu'on peut écrire

$$\frac{\sin \operatorname{am} m v}{\sin \operatorname{am} v} = \frac{\Pi(x^4 - \alpha^4)}{\Pi(1 - \alpha^4 x^4)}, \quad \frac{\sin \operatorname{am} n v}{\sin \operatorname{am} v} = \frac{\Pi(x^4 - \beta^4)}{\Pi(1 - \beta^4 x^4)}.$$

De là et des deux formules (1.) et (2.) on tire

$$(3.) \quad n^{i(p-1)} \equiv \frac{\Pi(\alpha^4 - \beta^4)}{\Pi(1 - \beta^4 \alpha^4)} \pmod{m},$$

$$(4.) \quad m^{s(q-1)} \equiv \frac{\Pi(\beta^4 - \alpha^4)}{\Pi(1 - \alpha^4 \beta^4)} \pmod{n},$$

où il faut combiner chaque valeur de α avec chaque valeur de β . Le nombre de ces combinaisons étant $\frac{1}{4}(p-1)\frac{1}{4}(q-1)$, la seule inspection des formules (3.) et (4.) suffit pour en conclure immédiatement le théorème fondamental sur les résidus biquadratiques.

§. 3.

Remarques.

Pour démontrer la loi de réciprocité relative aux résidus cubiques, il n'y a qu'à mettre à la place de l'équation différentielle $dx = dv\sqrt{(1-x^3)}$ celle-ci $dx = dv\sqrt{(1-x^3)}$ ou celle-ci $dx = dv\sqrt{(x(1-x^3))}$; et au lieu de prendre des nombres complexes de la forme $a+bi$, il n'y a qu'à considérer des nombres qui se composent des racines de l'équation $\zeta^2 + \zeta + 1 = 0$; au reste la marche de la démonstration est parfaitement analogue à celle que nous venons de suivre pour les résidus biquadratiques. Par cette raison et comme nous croyons avoir exposé clairement l'esprit de notre méthode, nous remettons à une autre occasion l'examen plus détaillé et les recherches ultérieures que nous avons entreprises sur ces applications de l'algèbre à l'arithmétique. Nous traiterons alors surtout des résidus de puissances supérieures, dont les théorèmes fondamentaux dépendent de l'élimination de plusieurs variables entre trois ou un plus grand nombre d'équations algébriques.

Il se pourrait qu'on n'approuvât pas l'usage des fonctions circulaires et elliptiques dans les raisonnements arithmétiques; mais il y a à observer que ces fonctions n'y entrent que d'une manière pour ainsi dire *symbolique*, et qu'il serait possible de les en chasser complètement sans détruire la substance et le fond des démonstrations. Pour faire voir cela relativement aux résidus quadratiques, reprenons la congruence $q^{s(p-1)} \equiv C\Pi(\alpha^2 - \beta^2) \pmod{p}$, où toutes les lettres doivent avoir la même signification que dans le §. 1. Cette formule donnant le caractère quadratique de q par rapport à p , tout dépend essentiellement du signe du second membre. Si donc on met à la place des α et des β d'autres quantités α' , β' soumises à la seule condition que $\alpha'^2 - \beta'^2$ ait toujours le même signe que $\alpha^2 - \beta^2$, le produit $C\Pi(\alpha'^2 - \beta'^2)$ exprimera toujours par son signe le caractère de q . Nous sommes donc conduits à ce théorème remarquable:

„Si l'on construit une courbe fermée quelconque, mais symétrique „par rapport à deux axes perpendiculaires, de sorte qu'elle ait quatre parties

„congrus, dont les ordonnées vont en augmentant dans le premier quart: qu'on
 „divise alors la circonférence de cette courbe en p et en q parties égales et
 „qu'on désigne par α et par β resp. les ordonnées positives qui correspondent
 „à ces deux divisions, je dis que q sera ou ne sera pas résidu quadratique
 „de p selon que le produit $(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} \Pi(\alpha^2 - \beta^2) = \Pi(\beta^2 - \alpha^2)$ pour lequel
 „chaque valeur de α est à combiner avec chaque valeur de β , aura le signe
 „plus ou le signe moins.”

Ce théorème, dont la loi de réciprocité est une conséquence immédiate, peut se démontrer d'une manière purement arithmétique. Il existe quelque chose d'analogue mais plus compliquée pour les résidus cubiques et biquadratiques, et on peut dire que pour la démonstration des lois de réciprocité qui s'y rapportent, on n'a nullement besoin de la formule de multiplication des fonctions elliptiques. Cependant il ne paraît pas toujours préférable d'éviter dans les recherches arithmétiques les fonctions analytiques, surtout quand on voit à postériori qu'elles n'entrent pas essentiellement dans les démonstrations et qu'elles servent seulement à fixer les idées et à abrégéer les conclusions.

Berlin, 13. Février 1845.

Fac-simile einer Handschrift von Copernicus

Quo me in Christo pr et dno Domo clarissimr, accepi has r d v humanissimas
et admodu familiaris, qui buscu etia no designata est mittere ad lectore libroru
meorum epigramma elegans factu et ad rem, non meis meritis, sed r d v benevolentia
singulari, qua studiosos prosequi solet. Ipse yatu r d v titulu operi meo infastiguo
ppona, si modo dignu sit opus, quod a r d v exornari tantopere mereatur, quod tantu
dulcant me doctores offi aliqd, quibus absq deret. Ego vero singulari benevolentia
et affectu erga me sum, quo me prosequi no cessat r d v quatum in me est
promereri, eiq in omnibus qbus possim vti debro sperare et obsequi cupio
Ex frankburg 7^{mo} Junij 1591

E r d v

obsequatiss

Nicolaus Copernicus

