RÉSULTANT ET SYMBOLE DE LEGENDRE

Jean-Yves MÉRINDOL

Professeur de Mathématique à l'U.F.R. de Mathématique de Strasbourg

L'article qui suit est un exercice de style un peu paradoxal puisqu'il va en fait du compliqué au simple. L'enseignement scolaire et universitaire insiste depuis des décennies, et avec de très bonnes raisons, sur ce qui est **linéaire**. De l'élémentaire – la règle de trois – aux premières années d'université – les espaces vectoriels – beaucoup de temps est accordé à ces notions. Et on s'aperçoit que l'algèbre linéaire constitue de fait le cœur des programmes d'algèbre du CAPES ou de l'Agrégation.

Mais ceci a une conséquence curieuse. Des structures beaucoup plus naturelles sont mal explorées. C'est le cas des entiers, dont l'étude est reléguée à des rappels marginaux sur les PGCD – PPCM. Sans même parler de corps de nombres, l'arithmétique élémentaire n'est que rarement abordée.

On va, de façon légèrement obsessionnelle, montrer que pourtant bien des constructions devenues familières, grâce à l'habitude, sur les espaces vectoriels, se transfèrent sans grande peine en notions intéressantes, bien qu'élémentaires, sur $\mathbb{Z}$ et ses quotients. Le fil directeur va être l'explication en parallèle des propriétés principales de $\mathbb{Z}$ et de $\mathbf{k}[X]$. Ces deux anneaux sont les anneaux d'entiers de leur corps des fractions respectifs : $\mathbb{Q}$ et $\mathbf{k}(x)$. Les lecteurs les plus savants auront reconnu les exemples de base des *"corps globaux"*. L'analogie des propriétés arithmétiques des extensions finies de $\mathbb{Q}$ – les extensions de nombres – et les propriétés géométriques des extensions de $\mathbf{k}(x)$ – les corps de fonctions des courbes algébriques – est un principe systématiquement utilisé dès le $19^{\text{ème}}$ siècle mais dont la fécondité est remarquable et certainement riche d'encore bien des surprises.

On va voir dans la suite que, même à un niveau volontairement très élémentaire, on peut se persuader de cette fécondité.

Voici un exemple de résultat qui peut être surprenant mais qui devient naturel avec la démarche présentée ici.

Soit n un entier impair, supérieur ou égal à 3. On constate facilement qu'il existe, à rotation près, $\frac{n-1}{2}$ polygones réguliers à n côtés inscrits dans un cercle de rayon 1. On autorise les polygones étoilés et aussi ceux qui ne sont pas convexes. Notons

$\ell_1^2(n)$, ..., $\ell_{\frac{n-1}{2}}^2(n)$ les $\frac{n-1}{2}$ carrés des longueurs des côtés de ces polygones. Soit m un second entier impair et intéressons nous au réel $\prod_{s=1}^{\frac{n-1}{2}} \prod_{t=1}^{\frac{m-1}{2}} (\ell_s^2(n)-\ell_t^2(m))$.

Alors on peut prouver que ce produit vaut 0 (lorsque n et m ne sont pas premiers entre eux – ceci est facile) et ±1 sinon – ce qui est moins clair. Reste à comprendre la signification du signe. Lorsque m est premier, on peut montrer que l'on trouve +1 exactement lorsque n est un carré modulo m. Ainsi ce produit est ce qu'on appelle le symbole de Legendre – lorsque m est premier – ou plus généralement – pour m impair quelconque – le symbole de Jacobi (voir III pour les définitions). Ce résultat est dû à G. Eisenstein dans l'une de ses preuves de la loi de réciprocité quadratique.

Sources : Je ne connais pas de références développant systématiquement le point de vue qui suit. Mais deux séries d'articles m'ont influencé. Tout d'abord ceux de Pierre Cartier dans l'*"Enseignement mathématique"* 16 (1970) où il s'intéresse aux définitions de la signature en pensant aux résultats de Zolotareff. Ensuite ceux de Gotthold Eisenstein, notamment celui paru au Journal de Crelle 29 (1845) p.177–184, reproduit dans *"Mathematische Werke I"*, p.291–298, Chelsea Pub. 1989.

I. Les anneaux $\mathbb{Z}$ et k[X].

1. Idéaux et éléments inversibles.

L'une des conséquences des travaux, notamment en arithmétique et en géométrie du 19ème siècle est l'introduction des notions de base de l'algèbre commutative, par exemple celles d'anneau et d'idéal. Ce qu'on va en utiliser ici est extrêmement sommaire.

Si A est un anneau commutatif avec un élément unité, et a un élément de A, l'idéal **(a)**=$\{ab/b\in A\}$ est dit **principal**. Deux éléments a_1 et a_2 de A définissent le même idéal principal si et seulement si ils sont **associés** c'est à dire qu'il existe un élément inversible $\alpha\in A^\times$ tel que $a_1=\alpha a_2$. On vient au passage de noter $A^\times$ l'ensemble des éléments **inversibles**, et pas seulement non nuls, de A. On utilisera parfois la notation A^* pour désigner les éléments non nuls de A : $A^*=A-\{0\}$.

L'ensemble quotient $A-\{0\}/A^\times$, qui s'identifie aux idéaux principaux non nuls de A sera noté dans la suite $Div_+(A)$.

C'est un semi–groupe : il existe sur $Div_+(A)$ une loi de composition interne

(a)+**(b)**=**(ab)**=$\{\alpha\beta / \alpha\in$**(a)**$;\beta\in$**(b)**$\}$ (attention : ne pas confondre avec la somme usuelle des sous–ensembles de A).

Dans le cas de $\mathbb{Z}$, les éléments inversibles sont $\{\pm 1\}$ et le semi-groupe $\mathrm{Div}_+(\mathbb{Z})$ s'identifie naturellement à $\mathbb{N}$ muni de la multiplication. Pour $\mathbf{k}[X]$, les éléments inversibles forment le groupe $\mathbf{k}^*$ et il est usuel d'identifier $\mathrm{Div}_+(\mathbf{k}[X])$ aux polynômes *"unitaires"*, c'est à dire à ceux dont le coefficient dominant est $+1$.

Il est temps de rappeler que ces deux anneaux $\mathbb{Z}$ et $\mathbf{k}[X]$ sont **principaux**, c'est à dire que tous les idéaux sont du type rencontrés précédemment. Ceci résulte de la possibilité d'effectuer dans ces anneaux une **division euclidienne**.

2. Division euclidienne.

2.1. Les polynômes.

Si A et B sont deux polynômes avec B non nul, il existe deux polynômes R et Q appelés respectivement **reste** et **quotient** tels que $A=BQ+R$ avec R *"plus simple"* que B. Si l'on utilise la convention commode que le degré du polynôme nul est $-\infty$, donc strictement inférieur au degré de tout autre polynôme, on exige comme condition sur R que $\deg R<\deg B$. Ceci entraîne aussi l'unicité de Q et R. Notons une certaine compatibilité de cette division avec l'action des inversibles de $\mathbf{k}[X]$. Par exemple, si l'on divise λA par B (pour $\lambda\in\mathbf{k}[X]^\times$) on trouve comme quotient λQ et comme reste λR.

2.2. Les entiers.

Le cas des entiers est en apparence plus simple et il est traité dès le primaire. Ce n'est pas tout à fait vrai puisqu'alors on *"divise"* en général des entiers positifs. Si a et b sont deux entiers relatifs, il existe deux entiers r et q tels que $a=bq+r$. Si l'on exige que $0\le r<|b|$, on a alors l'unicité. Mais on vient de perdre alors la compatibilité, au sens de 2-1, à l'action des inversibles de l'anneau $\mathbb{Z}$.

Contrairement à ce que l'on croit souvent, la forme précédente de la division euclidienne n'est ni la seule, ni la meilleure. On peut par exemple exiger que $-\frac{|b|}{2} \le r < \frac{|b|}{2}$. On se rapproche de la compatibilité par multiplication de a par -1 mais un problème subsiste lorsque b est pair puisqu'on n'a alors pas unicité. Lorsque b est impair tout va bien. Pourquoi ce problème dans le cas de $\mathbb{Z}$ alors que la situation est plus simple pour $\mathbf{k}[X]$? La raison en est la suivante. Soit λ inversible dans l'un de ces anneaux. Alors pour tout B dans $\mathbf{k}[X]$, $1-\lambda$ n'est jamais diviseur de 0 dans le quotient $\mathbf{k}[X]/(\mathbf{B})$. En revanche $1-(-1)=2$ est diviseur de 0 dans $\mathbb{Z}/(\mathbf{b})$ si et seulement si b est pair.

Mais en fait, l'unicité dans la division euclidienne n'est pas indispensable pour ce que nous allons en faire. On se convaint de ceci en vérifiant que l'existence suffit à prouver qu'un anneau avec division euclidienne est principal, ou à décrire l'algorithme d'Euclide de recherche du PGCD. On pourra donc pour $\mathbb{Z}$ utiliser cette variante de la division

euclidienne a=bq+r avec $|r| \leq \frac{|b|}{2}$. Elle est d'ailleurs plus efficace pour les calculs de PGCD.

2.3. Il faut remarquer l'usage que l'on vient de faire de la relation d'ordre naturelle sur $\mathbb{Z}$, à propos de la division euclidienne. La relation d'ordre naturelle sur $\mathbb{N}$ est aussi utilisée pour k[X] puisqu'alors on compare les degrés des polynômes.

3. La structure des espaces quotients.

Le quotient d'un anneau par un idéal est encore un anneau. Mais nous allons utiliser une structure plus faible et malgré tout suffisante pour nos constructions.

3.1. k[X]/(B).

Ces quotients sont évidemment des **k**–espaces vectoriels de dimension finie. On rencontre même ainsi tous les espaces de ce type, à isomorphisme près. On peut donc utiliser sur ce quotient toutes les ressources de l'algèbre linéaire : endomorphismes, déterminants, ...

Mais on vient de faire implicitement un choix un peu curieux qui mérite quelques commentaires. En effet, on n'a gardé de l'anneau **k**[X] que deux opérations : la multiplication par $\mathbf{k}^*=\mathbf{k}[X]^\times$, et l'addition.

On a compris que la première de ces structures est dans le droit fil de nos préoccupations mais la seconde est embarrassante si l'on veut passer à $\mathbb{Z}$ puisque la structure d'anneau sur $\mathbb{Z}/(\mathbf{b})$ se déduit de la structure de groupe additif sur ce quotient. On ne peut donc garder la structure additive sur $\mathbb{Z}/(\mathbf{b})$ sauf à tout garder de la structure d'anneau, ce qui rigidifie bien trop la situation. Pour mieux comprendre ce point, il est nécessaire d'évoquer un peu la géométrie projective.

L'action de $\mathbf{k}^*=\mathbf{k}[X]^\times$ sur **k**[X] passe au quotient par (**B**) et donne une action par homothéties sur l'espace vectoriel quotient. Le quotient de cet espace vectoriel par $\mathbf{k}^*$ est par définition l'espace projectif associé. Les automorphismes de l'espace vectoriel **k**[X]/**(B)** passent eux aussi au quotient (on utilise ici seulement le fait que pour u linéaire $u(\lambda v)=\lambda u(v)$ si $\lambda \in \mathbf{k}^*$, l'addition ne jouant aucun rôle) et définissent le **groupe projectif linéaire** des homographies bijectives de l'espace projectif. Ce qu'on appelle le théorème fondamental de la géométrie projective est le fait que les bijections d'un espace projectif dans lui–même qui respectent les alignements sont, à partir de la dimension 2, à un automorphisme de **k** près, exactement ces homographies bijectives. Mais c'est un autre résultat, apparenté à celui–ci, qui va nous servir. Il faut pour cela utiliser un peu de géométrie algébrique.

L'espace projectif a une structure de *"**k**–variété algébrique"*. Pour le néophyte, peu importe le sens précis de ceci. Ce qui compte c'est le résultat suivant : les bijections d'un espace projectif dans lui–même respectant cette structure de *"**k**–variété algébrique"* forment un groupe qui est exactement le groupe projectif linéaire. Autrement dit, il n'y a pas vraiment besoin de l'addition pour définir le groupe projectif linéaire. Reste à savoir passer du groupe projectif linéaire au groupe linéaire lui–même. Ceci n'est pas très difficile – on doit faire ce qu'on appelle une extension centrale – mais puisque la construction exacte ne nous sera ici d'aucune utilité, on la passe sous silence.

Le célèbre *"programme d'Erlangen"* dû à Félix Klein, définit la géométrie comme l'étude du groupe des *"automorphismes"* d'un espace. Par exemple, de ce point de vue, dans le cas des espaces vectoriels, le plus important n'est pas la notion d'espace vectoriel en elle–même, mais les groupes linéaires. Et l'on vient de voir que ce groupe linéaire peut se définir en oubliant la structure additive. Le prix à payer en est d'introduire le formalisme de la géométrie algébrique. Il est temps de passer à $\mathbb{Z}$, où ce formalisme sophistiqué est fort heureusement inutile.

3.2. $\mathbb{Z}/(b)$

Ce qui précède suggère de ne s'intéresser qu'à une chose : l'action de la multiplication par (–1) sur ce quotient. Il est de bon sens de croire que sur un ensemble fini, il n'y a pas lieu de se préoccuper de savoir quelle est la structure algébrique analogue à une *"**k**–variété algébrique"*. Nous sommes heureusement dans une situation assez élémentaire pour que ce bon sens nous suffise.

Ainsi l'on est conduit à considérer que l'analogue d'un espace vectoriel est un ensemble fini E muni d'une involution σ:E→E. On va dans la suite essentiellement s'intéresser à $\mathbb{Z}/(b)$ muni de l'involution qui est la multiplication par (–1). Lorsque b est impair, cette involution n'a qu'un point fixe : 0. Ce que l'on va utiliser comme analogue d'un **k**–espace vectoriel est un ensemble fini E (qui sera dans les exemples $\mathbb{Z}/(b) - \{0\}$ avec b impair) muni d'une involution σ **sans points fixes**. Le groupe des automorphismes de (E,σ) sera par définition l'ensemble des bijections de E dans E **commutant** à σ. L'ensemble des endomorphismes de E est l'ensemble des applications, bijectives ou non, de E dans E, commutant à σ.

II. Signature et déterminant.

1. Que le déterminant et la signature soient parents est bien connu. Ceci se retrouve d'ailleurs dès les définitions. Mais une solution alternative aux définitions classiques s'offre à nous pour définir la signature en utilisant le contexte introduit en I–3–2.

Prenons donc un ensemble E de cardinal pair muni d'une involution σ sans point fixe.

Définition 1 : Une *"base"* de cet espace E est un sous ensemble B de E tel que E soit l'union disjointe de B et $\sigma(B)$.

Mise en garde : ceci n'a bien sûr rien à voir avec la notion de base au sens des $\mathbb{Z}$–modules. Rappelons encore une fois que l'on ignore délibérément la structure additive sur E si il en existe par hasard une. Par ailleurs, l'ensemble B n'est pas ordonné, contrairement aux bases des espaces vectoriels.

Définition 2 : Soient (E,σ) et (F,τ) deux ensembles finis munis chacun d'une involution sans points fixes.
Soit $f:E\to F$ une application telle que $f\circ\sigma=\tau\circ f$.
On choisit une *"base"* B de E et une *"base"* C de F.
Si f n'est pas une bijection, posons $\varepsilon_{B,C}(f)=0$.
Si f est une bijection, posons $\varepsilon_{B,C}(f)=(-1)^{l_{(B,C)}(f)}$, où $l_{(B,C)}(f)$ est le cardinal de $\{b\in B/f(b)\notin C\}$.
On dira que $\varepsilon_{B,C}(f)$ est la signature de f, dans les bases B et C.

On peut démontrer une formule sur le comportement de $\varepsilon_{B,C}$ par changement de base, analogue à celle concernant le déterminant. On se contentera pour la suite du résultat suivant :

Proposition 1 : Soit (E,σ) un ensemble fini muni d'une involution σ sans point fixe. Soit $f:E\to E$ commutant à σ. alors la parité de $l_{B,B}(f)$ ne dépend pas du choix de la *"base"* B de E.

Preuve (indication) : Soit B' une autre *"base"* de E. On dira que B' est contiguë à B s'il existe un $b\in B$ tel que $B'=(B-\{b\})\cup\{\sigma(b)\}$.

Il suffit de prouver la propriété voulue sur deux *"bases"* contiguës puis de raisonner de *"proche en proche"*. On laisse au lecteur le soin de le faire, ou de s'en convaincre par un exemple. On note dans la suite $\varepsilon(f)$ pour $\varepsilon_{B,B}(f)$.

Proposition 2 : $\varepsilon(f)$ est égal à la signature de τ.

Preuve : On a utilisé la convention commode que la signature d'une application non bijective de E dans E est 0.

Si f est une bijection, la décomposition de f en cycles disjoints est de forme particulière à cause de l'égalité $\sigma\circ f=f\circ\sigma$. On peut énumérer les cycles ainsi :

$C_1, C_2, \ldots, C_p, D_1, D_2, \ldots, D_q, \overline{D_1}, \overline{D_2}, \ldots, \overline{D_q}$ où les C_i sont invariants par σ alors que σ échange D_j et $\overline{D_j}$.

En particulier chaque C_i est de longueur paire et peut s'écrire :

$$(a^i_1, \ldots, a^i_{n_i}, a^i_{n_i+1}, \ldots, a^i_{2n_i}) \text{ où } a^i_{n_i+p}=\sigma(a^i_p) \quad 1\leq p\leq n_i.$$

Choisissons comme base B celle qui contient le support de D_i et les n_i premiers éléments de $a^i_1, \ldots, a^i_{n_i}$ du support de C_i.

Il est alors clair que chaque Dj et chaque $\overline{D_j}$ contribue pour 0 à $\mathbf{l_{B,B}}(f)$. Par contre C_i contribue exactement pour 1 à $\mathbf{l_{B,B}}(f)$ (l'élément $a^i_{n_i}$ de B devenant $a^i_{n_i+1}$ de $\sigma(F)$).
Alors $\varepsilon(f)=(-1)^p=\text{sgn}(C_1)\times\ldots\times\text{sgn}(C_p)$ [car chaque C_i est de longueur paire, donc de signature (-1)].

$\varepsilon(f)=\text{sgn}(C_1)\times\ldots\times\text{sgn}(C_p)\times\text{sgn}(D_1)\times\text{sgn}(\overline{D_1}\times\ldots\times\text{sgn}(D_q)\times\text{sgn}\,\overline{D_q}$ [la longueur de D_j vaut celle de $\overline{D_j}$, donc ces deux cycles ont même signature]. D'où $\varepsilon(f)=\text{sgn}(f)$.

On va noter désormais $S_\sigma(E)$ le groupe (pour la composition) des automorphismes de E qui commutent à σ.

Proposition 3 : l'application $\varepsilon: S_\sigma(E)\to\{\pm 1\}=\mathbb{Z}^\times$ est un morphisme de groupe.

Preuve : Prenons deux éléments τ_1 et τ_2 dans $S_\sigma(E)$. Il est facile de vérifier que, si B est une *"base"* alors $f\in(\tau_1\tau_2 B)\cap\sigma B$ si et seulement si :
- soit $f\in(\tau_2 B)\cap(\sigma B)$ et $f\notin(\tau_1 B)\cap(\sigma B)$
- soit $f\in(\tau_1 B)\cap(\sigma B)$ et $f\notin(\tau_2 B)\cap(\sigma B)$

De là on tire que $l(\tau_1\tau_2)+l(\tau_1)+l(\tau_2)$ est pair et donc que ε est un morphisme de groupes.

Remarques :

1. Si A est un ensemble fini quelconque, et $\tau: A\to A$ une bijection, on peut considérer la bijection associée
   $\tau\times\tau : A\times A\to A\times A$.
   Soit $S=A\times A-\Delta$ (où Δ est la diagonale du produit).
   Cet ensemble est muni d'une involution sans point fixe : σ échange simplement les deux facteurs. On se ramène ainsi à la théorie précédente puisque $\tau\times\tau$ commute à σ. On retrouve ainsi une des définitions usuelles de la signature comme parité du nombre d'inversions d'une permutation.
   Il est rassurant de constater que la signature de la bijection τ est égale à la signature de $\tau\times\tau$ restreint à S. On peut le montrer en vérifiant d'abord que la signature de $\tau\times\tau$ sur $A\times A$ est toujours +1, puis en remarquant que $A\times A$ est

l'union disjointe de S et de Δ et que la restriction de $\tau\times\tau$ à Δ s'identifie à l'action de τ sur A.

2. Si E a n éléments, avec n impair, et est muni d'une involution σ ayant un point fixe 0, le nombre d'éléments d'une *"base"* de $E-\{0\}$ est $\frac{n-1}{2}$. Ce nombre est l'analogue de la dimension, pour E ou $E-\{0\}$. On peut d'ailleurs vérifier que $\varepsilon(\sigma)=(-1)^{\frac{n-1}{2}}$, ce qui est à rapprocher du fait que le déterminant de la multiplication par λ dans un $\mathbf{k}$–espace vectoriel de dimension n est $(\lambda)^n$.

III. Résultant de Sylvester et symbole de Legendre–Jacobi.

3.1. Le cas des polynômes.

Voici l'une des définitions les plus usuelles du résultant de deux polynômes P et Q de degrés respectifs p et q. Si n est un entier, on note $\mathbf{k}[X]_n$ l'espace vectoriel des polynômes dont le degré est inférieur ou égal à n. Cet espace vectoriel a une base *"canonique"* : X^n, X^{n-1}, ..., 1 (attention à l'ordre!).

Soit φ : $\mathbf{k}[X]_{q-1}\times\mathbf{k}[X]_{p-1} \rightarrow \mathbf{k}[X]_{p+q-1}$ l'application linéaire définie par $\varphi(U,V)=UP+VQ$.

Bien que φ ne soit pas un endomorphisme, on peut malgré tout s'intéresser à son déterminant. On utilise pour cela les bases de $\mathbf{k}[X]_n$ (n=q–1, p–1 et p+q–1) que l'on vient de signaler ci–dessus, ce qui nous donne aussi une base du produit $k[X]_{q-1}\times k[X]_{p-1}$.

Définition 1 : Le résultat noté Res(P,Q) est le déterminant de la matrice de φ dans les bases introduites ci–dessus.

Grâce au théorème de Bézout, $Res(P,Q)\neq 0$ si et seulement si P et Q sont premiers entre eux. Remarquons aussi que si les coefficients de P et Q sont dans un sous–anneau A de $\mathbf{k}$, alors Res(P,Q) appartient à A. On utilisera ceci plus loin dans le cas $A=\mathbb{Z}\subset\mathbb{Q}=\mathbf{k}$. Il est plus agréable, et naturel, d'utiliser une variante de cette définition. En effet on a, pour tout polynôme N de degré n, un isomorphisme naturel entre $\mathbf{k}[X]/(N)$ et $\mathbf{k}[X]_{n-1}$.

Définition 2 : Res(P,Q) est le déterminant de l'application ψ.
ψ : $\mathbf{k}[X]/(Q)\times\mathbf{k}[X]/(P)\rightarrow\mathbf{k}[X]/(PQ)$
où ψ est l'application linéaire induite par $(U,V)\rightarrow UP+VQ$.

Les bases utilisées maintenant pour définir le déterminant de ψ sont celles obtenues par image dans les quotients, de $\{X^n, X^{n-1}, ..., X, 1\}$ (pour le *"bon"* n). Autrement dit, on munit chaque quotient de la forme volume provenant de celle de $\mathbf{k}[X]$ définie par $\{..., X^n, ..., X, 1\}$.

Remarquons aussi que l'application ψ est très classique. Il s'agit de celle utilisée dans le *"lemme des restes chinois"*. De façon précise ce lemme énonce que si P et Q sont premiers entre eux, alors ψ est un isomorphisme de groupes additifs (on a aussi un isomorphisme d'anneaux, mais qui n'est pas donné par ψ).

Proposition (loi de réciprocité) : $\mathrm{Res}(P,Q)=(-1)^{\deg P.\deg Q}.\mathrm{Res}(Q,P)$.

La preuve est évidente (compter combien on échange de colonnes).

Cette définition permet, lorsque P est unitaire, d'obtenir une caractérisation agréable du résultant.

Proposition 1 : Si P est unitaire, le résultant de P et Q, Res(P,Q) est égal au déterminant de l'endomorphisme de $\mathbf{k}[X]/(P)$ induit par la multiplication par Q.

Preuve : On a une application naturelle obtenue par multiplication par P :

$$\mathbf{k}[X]/(Q) \xrightarrow{\times P} \mathbf{k}[X]/(PQ)$$

Le quotient de $\mathbf{k}[X]/(Q)$ par l'image $P\times\mathbf{k}[X]/(Q)$ s'identifie naturellement à $\mathbf{k}[X]/(P)$.

Considérons θ : $\mathbf{k}[X]/(Q)\times\mathbf{k}[X]/(P) \to \mathbf{k}[X]/(PQ)$ définie par $\theta(U,V)=UP+V$. Il est facile de vérifier que, dans les bases *"canoniques"*, θ a une matrice qui est triangulaire inférieure et dont les éléments diagonaux sont tous égaux à 1 (on utilise ici que P est unitaire). Ainsi $\det(\theta)=1$ et θ est bijectif.

Posons $\psi_0=\psi\circ\theta^{-1}$: $\mathbf{k}[X]/(PQ) \to \mathbf{k}[X]/(PQ)$

Explicitement, si $U\in\mathbf{k}[X]/(Q)$ et $V\in\mathbf{k}[X]/(P)$ alors $\psi(UP+V)=UP+VQ$.

Cette formule montre que ψ_0 se restreint en l'identité sur l'image de $\mathbf{k}[X]/(Q) \xrightarrow{\times P} \mathbf{k}[X]/(PQ)$ et donne la multiplication par Q sur le quotient $\mathbf{k}[X]/(P)$.

Ainsi $\det(\psi_0)=\det($ multiplication par Q dans $\mathbf{k}[X]/(P))$

$$=\det(\psi_0\circ\theta^{-1})=\det\psi_0.\det(\theta)^{-1}=\mathrm{Res}(P,Q).$$

Corollaire :

$$\mathrm{Res}(P_1P_2,Q)=\mathrm{Res}(P_1,Q).\mathrm{Res}(P_2,Q).$$
$$\mathrm{Res}(P,Q_1Q_2)=\mathrm{Res}(P,Q_1).\mathrm{Res}(P,Q_2).$$

Preuve : la première assertion résulte de la seconde grâce à la loi de réciprocité. La seconde est claire si P est unitaire grâce au résultat de la proposition 1. Si $P=aP$ avec P unitaire, il est évident que pour tout R, $res(P,R)=a^{degR}Res(P,R)$.
Ceci permet de terminer la preuve du corollaire.

3.2. Le cas des entiers.

On souhaite ici montrer que le symbole de Legendre–Jacobi est l'analogue, dans le cas des entiers, du résultant.

Rappelons d'abord sa définition la plus classique. Commençons par le symbole de Legendre. Soit q un **premier** positif de $\mathbb{Z}$ autre que 2. On s'intéresse, pour n un entier que ne divise pas q, à savoir si n est, ou n'est pas, un carré modulo q. On définit ainsi $\left(\frac{n}{q}\right)$:

$$\left(\frac{n}{q}\right) = \begin{cases} +1 \text{ si n est un carré modulo q} \\ -1 \text{ si n n'est pas un carré modulo q} \end{cases}$$

Il est souvent commode, lorsque n est divisible par q, de poser $\left(\frac{n}{q}\right)=0$.

Dans cette définition, n et q jouent des rôles extrêmement dissymétriques. Le célèbre résultat qui suit n'en est que plus frappant.

> **Théorème** (loi de réciprocité) : Soient p et q deux nombres premiers strictement supérieurs à 2.
> Alors $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$

Ce résultat a été deviné par Legendre puis pleinement établi par Gauss qui a su en donner de multiples preuves. On renvoie à l'ouvrage de Bachmann cité en référence pour donner un historique des diverses méthodes utilisées au $19^{ème}$ siècle pour prouver ce résultat.

On peut étendre la définition du symbole de Legendre de la façon suivante. Soient n et m deux entiers, avec m strictement positif. On suppose que $m=p_1...p_k$ est la décomposition de m en produits de facteurs premiers, éventuellement répétés, alors on pose, pour m **impair**, $\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right) \cdots \left(\frac{n}{p_k}\right)$. C'est le symbole de Jacobi.

Il est plus délicat de définir $\left(\frac{n}{m}\right)$ pour m pair. On peut néanmoins le faire, mais comme ceci n'aura pas d'importance ici, on renvoie à l'un des ouvrages cités. On peut aussi

définir $\left(\frac{n}{m}\right)$ pour m négatif mais il y a dans la littérature plusieurs conventions de signes contradictoires qui sont utilisées.

La loi de réciprocité quadratique s'étend aux symboles de Jacobi.

Théorème : Soient m et n deux entiers positifs impairs.
Alors $\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}} \left(\frac{m}{n}\right)$

On peut aussi énoncer une loi de réciprocité un peu plus compliquée, si n ou m est pair.

Un résultat très simple, dû à L. Euler, est à signaler :

Proposition (L. Euler) : Si q est un entier impair premier,
$\left(\frac{n}{q}\right) = n^{\frac{q-1}{2}} [q]$

Preuve : Si $n \equiv 0$ [q], le résultat est trivial. Sinon soit $x \in (\mathbb{Z}/q\mathbb{Z})^*$ la classe de n, modulo q. Le groupe multiplicatif a q−1 éléments et d'après le résultat élémentaire de Lagrange, $x^{q-1}=1$.

En particulier si n est un carré modulo q, $x=y^2$ et $x^{\frac{q-1}{2}}=y^{q-1}=1=\left(\frac{n}{q}\right)$.

Mais le polynôme $X^{\frac{q-1}{2}}-1$ a au plus $\frac{q-1}{2}$ racines dans le corps $\mathbb{Z}/q\mathbb{Z}$. On vient de voir qu'il avait comme racines les $\frac{q-1}{2}$ classes de carrés (il y a bien $\frac{q-1}{2}$ telles classes, comme le montre le fait que le noyau de l'automorphisme θ de $(\mathbb{Z}/q\mathbb{Z})^*$ qui à y associe y^2 est composé des deux éléments $\{\pm 1\}$). Il n'a donc aucune autre racine et si n n'est pas un carré modulo q, $(n^{\frac{q-1}{2}})^2 \equiv 1$ entraîne que $n^{\frac{q-1}{2}} \equiv -1$. Ceci prouve le résultat d'Euler.

Corollaire : Si n_1, n_2 et m sont des entiers impairs positifs,
$$\left(\frac{n_1 n_2}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_2}{m}\right)$$
$$\left(\frac{m}{n_1 n_2}\right) = \left(\frac{m}{n_1}\right)\left(\frac{m}{n_2}\right)$$

Preuve : La seconde formule résulte de la définition même du symbole de Jacobi. Pour prouver la première formule, on utilise d'abord la définition pour se ramener au symbole de Legendre puis on utilise le résultat de L. Euler.

Ainsi, si q impair premier est fixé, le symbole de Legendre est un morphisme du groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$ vers $\{\pm 1\} = \mathbb{Z}^\times$. C'est en fait le seul morphisme non constant

entre ces groupes. Pour démontrer ceci on peut évoquer le fait bien connu que le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$ est un groupe cyclique, ce qui entraîne qu'il admet un seul sous groupe d'indice 2.

Corollaire 1 (Zolotareff) : Soit q un nombre premier impair positif. Soit n un entier. Le symbole de Legendre $\left(\frac{n}{q}\right)$ est égal à la signature de l'application de $\mathbb{Z}/q\mathbb{Z}$ dans lui-même induite par la multiplication par n.

Preuve : Si n est divisé par q, cette application n'est pas une bijection. La signature vaut alors 0, tout comme le symbole de Legendre.

Sinon on a une application naturelle de $(\mathbb{Z}/q\mathbb{Z})^*$ vers $\{\pm 1\}$ qui à la classe x de n associe la signature de la multiplication par n.

L'associativité de la multiplication montre que cette application est un morphisme de groupes. Reste à voir qu'il n'est pas trivial afin de montrer qu'il s'agit bien du symbole de Legendre. On laisse au lecteur le soin de la vérifier en s'intéressant par exemple au cas où x est un générateur de groupe cyclique $(\mathbb{Z}/q\mathbb{Z})^*$ (alors la permutation induite par x est le cycle $(x, x^2, ..., x^{q-1})$ qui ayant q−1 éléments a comme signature $(-1)^q=-1$).

On constate que l'on vient de retrouver l'exact analogue de la proposition 1 précédente qui, elle, portait sur les résultants de polynômes.

Avant de continuer, il est agréable de remarquer qu'en utilisant le formalisme du II sur la signature, et en remarquant que la multiplication par n dans $\mathbb{Z}/q\mathbb{Z}$ commute à la multiplication par −1, on obtient le résultat suivant :

Corollaire 2 (C.F. Gauss) : Soit q un nombre premier impair positif. Soit n un entier non divisible par q. Considérons les $\frac{q-1}{2}$ entiers $\left\{n, 2n, ..., \frac{q-1}{2}\right\}$. Faisons la division euclidienne de ces entiers par q comme en II.2. On trouve alors $\frac{q-1}{2}$ restes tous compris entre $-\left(\frac{q-1}{2}\right)$ et $+\left(\frac{q-1}{2}\right)$. Alors $\left(\frac{n}{q}\right)$ vaut $(-1)^s$ où s est le nombre de restes négatifs.

Il est maintenant tentant d'essayer de définir le symbole de Jacobi comme l'est le résultant. Soient p et q deux entiers impairs. L'idée naïve est de s'intéresser à l'application $\varphi : \mathbb{Z}/(q)\times \mathbb{Z}/(p)\to \mathbb{Z}/(pq)$ définie par $\varphi(u,v)=up+vq$ (Bézout). Il s'agirait donc de donner un sens à la signature de φ qui est, lorsque p et q sont premiers entre eux, une bijection entre deux ensembles différents.

Pour pouvoir le faire de façon naïve, il faudrait décrire une *"base"* naturelle de l'ensemble produit $(\mathbb{Z}/(q))^*\times(\mathbb{Z}/(p))^*$. On a bien sûr une *"base"* naturelle de chacun des facteurs, il s'agit de celle qui est constituée de l'image des $\frac{q-1}{2}\left(\text{resp. } \frac{p-1}{2}\right)$ premiers entiers positifs. Mais il n'est pas si évident d'obtenir une base du produit. Notons que celui-ci est bien sûr de cardinal $(p-1)(q-1)$ et qu'une base du produit devrait avoir $\frac{(p-1)(q-1)}{2}$ éléments. On n'est en fait plus dans la situation proche de celle des espaces vectoriels (ou la dimension d'un produit vaut la somme des dimensions des facteurs). On est plus proche du produit tensoriel des espaces vectoriels. Mais on aimerait alors avoir plutôt une dimension valant $\frac{p-1}{2}\frac{q-1}{2}$ et le produit usuel des ensembles ne convient pas.

On se convainc assez vite que l'analogue du produit (ou si l'on préfère de la somme directe) des espaces vectoriels est l'union disjointe. Il se trouve que nous n'utiliserons pas dans la suite cette construction et nous laissons le soin au lecteur de la développer si il le souhaite. Notons seulement que l'algèbre des fonctions sur l'union disjointe de deux ensembles finis est bien la somme directe de chacune des algèbres de fonctions sur chacun de ces ensembles, ce qui justifie ce point de vue.

On va plutôt dans la prochaine partie utiliser l'analogue du produit tensoriel. Soient donc E et F deux ensembles finis munis d'involutions sans points fixes notées toutes les deux par $x\to -x$.

Le groupe $\mathbb{Z}/(2)\times\mathbb{Z}/(2)$ agit alors sur le produit $E\times F$ (c'est l'action usuelle du groupe de Klein) en envoyant (x,y) sur $(\pm x,\pm y)$.

On peut définir trois quotients naturels :

$$E\overset{d}{\times}F = E\times F/(x,y)\sim(x,-y) \qquad \text{(droite)}$$

$$E\overset{g}{\times}F = E\times F/(x,y)\sim(-x,y) \qquad \text{(gauche)}$$

et $$E\overset{c}{\times}F = E\times F/(x,y)\sim(-x,-y) \qquad \text{(centre)}$$

Chacun de ces quotients est muni d'une involution sans point fixe correspondant à l'*"autre"* action de $\mathbb{Z}/(2)$. Par exemple pour les deux premiers produits $\overset{d}{\times}$ et $\overset{g}{\times}$, il s'agit de l'involution qui associe à la classe de (x,y) la classe de $(-x,-y)$.

Il est alors facile de vérifier que si E est muni d'une base B et F d'une base C, les produits $E\overset{d}{\times}F$, $E\overset{g}{\times}F$ et $E\overset{c}{\times}F$ sont tous munis d'une base qui est l'image dans ces quotients de $B\times C$.

Exercice :

1. constater que $\dim(E \overset{d}{\times} F)=\dim(E \overset{g}{\times} F)=\dim(E \overset{c}{\times} F)=\dim E.\dim F$.

2. Soit e (resp. f) une permutation de E (resp. F) commutant à l'involution. Définir alors des permutations $e \overset{d}{\times} f$, $e \overset{g}{\times} f$ et $e \overset{c}{\times} f$ commutant aux involutions sur les quotients. Vérifiez que la signature de ces permutations est $\mathrm{sgn}(e)^{\dim F} \times \mathrm{sgn}(f)^{\dim E}$.

Nous pouvons revenir aux entiers et utiliser dans la partie suivante les formalismes qui viennent d'être introduits.

IV. Diverses autres définitions du symbole de Legendre–Jacobi.

On va maintenant utiliser les parties II et III afin de retrouver diverses formules donnant le symbole de Jacobi.

Les démonstrations seront souvent seulement rapidement évoquées et les détails – pas toujours évidents – laissés en exercice.

Dans toute la suite p et q représentent deux entiers positifs impairs supérieurs ou égaux à trois. On ne suppose **pas** que ces entiers soient premiers.

4.1. Zolotareff.

Proposition 1 : la signature de l'application de $\mathbb{Z}/(q)$ dans lui–même induite par la multiplication par p est égale au symbole de Jacobi $\left(\frac{p}{q}\right)$.

Indication de la preuve : Si q est premier, ce résultat a été prouvé en III. Sinon, on décompose q en produit de facteurs premiers : $q=q_1^{\alpha_1}...q_r^{\alpha_r}$.
Alors $\mathbb{Z}/(q)$ est isomorphe comme anneau au produit $\mathbb{Z}/(q_1^{\alpha_1}) \times ... \times \mathbb{Z}/(q_r^{\alpha_r})$.

On laisse au lecteur le soin de montrer que la signature de la multiplication par p dans $\mathbb{Z}/(q_i^{\alpha_i})$ est bien $\left(\frac{p}{q_i}\right)^{\alpha_i}$, ce qui termine la preuve de la proposition.

4.2. Kronecker.

Le théorème des restes chinois nous apprend que, lorsque p et q sont premiers entre eux, il existe un isomorphisme θ d'anneaux – en fait unique – entre $\mathbb{Z}/(q) \times \mathbb{Z}/(p)$ et $\mathbb{Z}/(pq)$. On a un autre isomorphisme, mais cette fois seulement de groupes, entre $\mathbb{Z}/(q) \times \mathbb{Z}/(p)$ et $\mathbb{Z}/(pq)$ défini par $\varphi(u,v)=up+vq$.

Dans ces deux isomorphismes, le sous–ensemble $(\mathbb{Z}/(q))^* \times (\mathbb{Z}/(p))^*$ s'envoie sur la même partie de $\mathbb{Z}/(pq)$. On va la noter $(\mathbb{Z}/(pq))^{**}$. Par exemple si p et q sont premiers tous les deux, $(\mathbb{Z}/(pq))^{**}$ est simplement $(\mathbb{Z}/(pq))^\times$. Mais en général $(\mathbb{Z}/(pq))^{**}$ dépend non seulement de pq mais aussi du choix de p et de q. Cet ensemble a toujours $(p-1)(q-1)$ éléments.

Mais on a sur $(\mathbb{Z}/(q))^* \times (\mathbb{Z}/(p))^*$ et, par transport sur $(\mathbb{Z}/(pq))^{**}$, une action de groupe de $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ donnée par les involutions sur chaque facteur.

On peut donc utiliser la construction signalée à la fin du III et définir par exemple $(\mathbb{Z}/(q))^* \overset{d}{\times} (\mathbb{Z}/(p))^*$. Posons $t=\theta(1,-1)$. C'est un élément de $(\mathbb{Z}/(pq))^{**}$ et la multiplication par t est une involution sans points fixes de $(\mathbb{Z}/(pq))^{**}$. Définissons enfin $(\mathbb{Z}/(pq))^{**d}$ comme le **quotient** de $(\mathbb{Z}/(pq))^{**}$ par la multiplication par t.

D'après les constructions mêmes, l'application de Bézout φ, passe au quotient et donne une bijection que l'on va noter φ^d entre

$$(\mathbb{Z}/(q))^* \overset{d}{\times} (\mathbb{Z}/(p))^* \text{ et } (\mathbb{Z}/(pq))^{**d}.$$

Ces deux ensembles sont encore munis d'une involution sans points fixes qui est simplement la multiplication par (-1) et φ^d commute à ces involutions.
Le premier ensemble est muni d'une base naturelle qui est donnée par les couples, ou plutôt leurs classes, (u,v) avec $0<u\leq\frac{q-1}{2}$, $0<v\leq\frac{p-1}{2}$.

Notons enfin que, puisque dans le *"produit"*

$$(\mathbb{Z}/(q))^* \overset{d}{\times} (\mathbb{Z}/(p))^* \quad (u,v)=(u,-v),$$
$$\varphi^d(u,v)=up+vq=up-vq \text{ dans } (\mathbb{Z}/(pq))^{**d}.$$

On est maintenant dans une situation ou le résultat suivant devient assez naturel.

> **Théorème** (L. Kronecker) : Considérons l'ensemble S des entiers de la forme $up-vq$ où $u\in\left\{1,2,\ldots,\frac{q-1}{2}\right\}$ et $v\in\left\{1,2,\ldots,\frac{p-1}{2}\right\}$. Soit s le nombre des entiers de S qui sont négatifs. Alors $(-1)^s=\left(\frac{p}{q}\right)$

Indication de la preuve : Il s'agit essentiellement d'interpréter ce signe $(-1)^s$ en utilisant les notions que l'on vient d'introduire. Ce qu'il faut d'abord clairement faire, c'est décrire

une *"base naturelle"* de l'ensemble $(\mathbb{Z}/(pq))^{**d}$ provenant essentiellement de la base $\mathbb{N}^* \subset \mathbb{Z}^*$.

Il s'agit donc de décrire des représentants des classes du quotient $(\mathbb{Z}/(pq))^{**}/\{\pm 1,\pm 1\}$. Mais $(\mathbb{Z}/(pq))^{**}$ ou une *"base naturelle"* pour l'action de $\{\pm 1\}$ constituée des $\frac{(p-1)(q-1)}{2}$ éléments non divisibles par p ou par q entre 1 et $\frac{pq-1}{2}$.

On constate, ce qui est rassurant dans l'analogie avec les résultants, que l'on utilise de façon essentielle les entiers **positifs**, c'est à dire indirectement l'ordre sur $\mathbb{Z}$.

Reste maintenant à passer au quotient par t. Le plus simple est de constater que les couples d'éléments (x,−x) de $(\mathbb{Z}/(pq))^{**d}$ sont en bijection avec les éléments de l'image $\varphi^d\left(\left\{1,2,\ldots,\frac{q-1}{2}\right\}\times\left\{1,2,\ldots,\frac{p-1}{2}\right\}\right)$. Les éléments de cette image se relèvent en les entiers $up-vq\left(u\in\left\{1,2,\ldots,\frac{q-1}{2}\right\},v\in\left\{1,2,\ldots,\frac{p-1}{2}\right\}\right)$, entiers tous compris entre $-\frac{pq-1}{2}$ et $+\frac{pq-1}{2}$

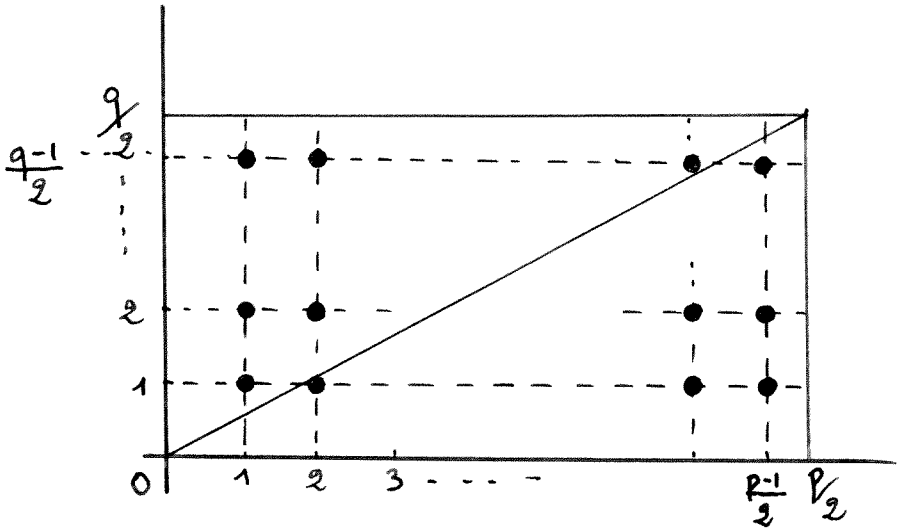
Ceci conduit à prendre comme *"base naturelle"* de $(\mathbb{Z}/(pq))^{**d}$, les $\frac{(p-1)}{2}\times\frac{(q-1)}{2}$ valeurs absolues de ces entiers $|up-vq|$.

> **Exemple** : p=5, q=7
> up−vq prend les valeurs −9, −4, −2, 1, 3, 8.
> La base naturelle choisie est 1, 2, 3, 4, 8, 9.
> Notons que t=−6 (−6≡1[7] et −6≡−1[5]) et que 6t=1, 11t=4, 12t=−2, 13t=8, 16t=−9 et 17t=3. Donc les six autres éléments non divisibles par 5 ou par 7 entre 1 et $\frac{pq-1}{2}=17$ sont bien dans l'orbite de la base naturelle pour l'action de $\{\pm 1,\pm t\}$.

Alors $(-1)^s$ est la *"signature"* de φ^d calculée dans les bases que l'on vient d'introduire. Ce qui rend plausible, sans le prouver, le résultat annoncé.

Problème : prouver ce résultat en s'inspirant de la preuve de la proposition 1 de III.1. Il faudra ici partir du résultat du à Zolotareff et arriver au résultat du théorème, c'est à dire renverser la preuve donnée en III.1.

Interprétation géométrique : Soient p et q premiers entre eux. Considérons le rectangle dessiné ci−dessous (de diagonale d'extremité l'origine et le point $\left(\frac{p}{2},\frac{q}{2}\right)$).



Le nombre de points entiers dans ce rectangle (à coordonnées strictement positives) est $\frac{p-1}{2}\frac{q-1}{2}$. La grande diagonale du rectangle le partage en deux triangles de mêmes surfaces. Mais ces deux triangles ne contiennent pas exactement le même nombre de points entiers.

Notons T(p,q) le nombre de points entiers dans le triangle inférieur. Puisque la diagonale a comme équation up−vq=0, T(p,q) est le nombre de solutions entières de :

$$up-vq<0 \qquad 0<u\leq\frac{p-1}{2} \qquad 0<v\leq\frac{q-1}{2}$$

Donc d'après le théorème qui précède, $\left(\frac{p}{q}\right)=(-1)^{T(p,q)}$. Ce résultat a été aussi établi par G. Eisenstein (1844).

Interprétation combinatoire : gardons encore p et q premiers entre eux.

Considérons les $\frac{p-1}{2}+\frac{q-1}{2}$ nombres distincts suivants, classés dans cet ordre :

$$q,\ 2q,\ \ldots,\ \frac{p-1}{2}q,\ p,\ 2p,\ \ldots,\ \frac{q-1}{2}p.$$

Cette suite doit être permutée pour être reécrite dans l'ordre croissant. La signature de la permutation nécessaire est $\left(\frac{p}{q}\right)$. En effet, pour calculer cette signature, il suffit de calculer le nombre d'inversions à effectuer. Mais puisque la sous−suite $q,\ 2q,\ \ldots,\ \frac{p-1}{2}q$ est croissante, ainsi que l'autre sous−suite $p,\ 2p,\ \ldots,\ \frac{q-1}{2}p$, il suffit de compter combien il y a de signes négatifs dans les différences up−vq, $\left(u\in\left\{1,2,\ldots,\frac{q-1}{2}\right\}\text{ et }v\in\left\{1,2,\ldots,\frac{p-1}{2}\right\}\right)$. On retrouve ainsi l'énoncé du théorème précédent.

Exercice : déduire de l'énoncé du théorème ou de l'une ou l'autre des interprétations des preuves immédiates de la loi de réciprocité quadratique.

Remarque : L'interprétation combinatoire est, en un certain sens, encore plus proche de la définition usuelle du résultant que l'énoncé du théorème de Kronecker. On a en effet ici une bijection entre deux ensembles différents comportant chacun $\frac{p-1}{2}+\frac{q-1}{2}$ éléments et $\left(\frac{p}{q}\right)$ est la signature de cette bijection. On a pu donner un sens à cette signature en utilisant l'ordre naturel sur $\mathbb{N}$. On retrouve bien là la définition usuelle du résultant qui utilise la somme directe k[X]/(Q)⊕k[X]/(P) (remplacée dans ce contexte par l'union disjointe $\mathbb{Z}/(q)\cup\mathbb{Z}/(p)$ plutôt que par le produit tensoriel k[X]/(Q)⊗k[X]/(p) (dont l'analogue ici est $\mathbb{Z}/(q)\overset{d}{\times}\mathbb{Z}/(p)$). Il est rassurant de noter que le résultant peut aussi se définir sur k[X]/(Q)⊗k[X]/(P)≈k[X,Y]/(Q(X),P(Y)) comme le déterminant de l'endomorphisme induit par multiplication par X−Y. Le lecteur souhaitant pousser les analogies aussi loin que possible est invité à méditer cette remarque.

V. Le symbole de Jacobi comme résultant.

Une parenté aussi forte laisse penser que le symbole de Jacobi peut même se calculer comme un résultant. C'est ce que l'on va montrer ici en se laissant guider par le travail fait en III.

Il est classique que la signature peut se voir comme un déterminant. Il suffit d'introduire les matrices de permutation. De façon explicite, si $\sigma : \{1,...,n\} \to \{1,...,n\}$ est une application, on définit la matrice $M(\sigma)=(a_{ij})$ ou $a_{ij}=0$ sauf si $i=\sigma(j)$, auquel cas $a_{ij}=1$. alors la définition même du déterminant (par exemple comme forme n−linéaire alternée) montre que $\det M(\sigma)=sgn(\sigma)$.

Le problème est d'associer à tout entier impair n positif un polynôme P_n tel que si m est impair, $\left(\frac{n}{m}\right)$ soit le résultant des deux polynômes P_n et P_m. La loi de réciprocité quadratique montre que le degré de P_n doit être $\frac{n-1}{2}$.

Le polynôme le plus naturellement lié à $\mathbb{Z}/(n)$ est celui qui vient de la division du cercle en n parties égales, c'est à dire celui qui permet le calcul des racines $n^{ièmes}$ de l'unité. Il s'agit de X^n-1. On sait que les racines complexes de ce polynôme forment un groupe μ_n (multiplicatif) cyclique d'ordre n, donc isomorphe (lorsqu'on choisit une racine primitive, c'est à dire un générateur) à $(\mathbb{Z}/(n),+)$

Le sous ensemble $(\mathbb{Z}/(n))-\{0\}$ est alors associé au polynôme $\frac{X^n-1}{X-1} = X^{n-1}+X^{n-2}+\ldots+1 = H_n(X)$. La multiplication par (-1) dans $(\mathbb{Z}/(n))-\{0\}$ donne le passage à l'inverse multiplicatif dans μ_n : $z \to \frac{1}{z}$. On constate que le polynôme $H_n(X)$ se comporte bien dans cette opération : $X^{n-1}H_n\left(\frac{1}{X}\right)=H_n(X)$.

Les considérations du III., notamment celles de la fin introduisant les produits $\overset{d}{\times}$, $\overset{g}{\times}$ et $\overset{c}{\times}$, montrent que l'on doit s'intéresser au quotient de $\mathbb{Z}/(n)-\{0\}$ par la multiplication par (-1), donc à ce qui est invariant par cette action.

En terme de polynômes, on est donc naturellement amené à s'intéresser au polynômes en $Y=X+\frac{1}{X}$.

Définition : On définit $Q_n(Y)$ comme le polynôme de $\mathbb{Z}[Y]$ vérifiant :

$$Q_n\left(X+\frac{1}{X}\right) = X^{\frac{n-1}{2}}+X^{\frac{n-3}{2}}+\ldots+X^{-\left(\frac{n-3}{2}\right)}+X^{-\left(\frac{n-1}{2}\right)} = X^{-\left(\frac{n-1}{2}\right)}H_n(X)$$

Ce polynôme est clairement de degré $\frac{n-1}{2}$. Le résultat suivant devient naturel :

Théorème : Si n et m sont deux entiers impairs positifs,

$$\left(\frac{n}{m}\right) = \mathrm{Res}(Q_m,Q_n) = \mathrm{Res}(Q_n(-X),Q_m(-X))$$

Preuve (indication) : Il est facile de montrer que Q_n et Q_m ont une racine commune dans un corps algébriquement clos **k** si et seulement si H_n et H_m ont une racine commune dans ce même corps. Mais les racines communes H_n et H_m sont simultanément des racines $n^{\text{ièmes}}$ et $m^{\text{ièmes}}$ de l'unité, autres que 1. Elles sont donc exactement les racines $d^{\text{ièmes}}$ de l'unité, autres que 1, où d est le pgcd de n et m. Ainsi $\mathrm{Res}(Q_m,Q_n)=0$ si et seulement si m et n ne sont pas premiers entre eux.

Mais, puisque Q_m et Q_n sont à coefficients entiers, le résultant est un entier (voir la remarque en 3.1. entre les définitions 1 et 2). Supposons désormais que m et n sont premiers entre eux. On va prouver que $\mathrm{Res}(Q_m,Q_n)=\pm 1$. Soit p un nombre premier. L'argument précédent prouve que les réductions modulo p de Q_m et Q_n n'ont aucunes racines communes dans une clôture algébrique **k** de $\mathbb{Z}/p\,\mathbb{Z}$. En particulier, la réduction modulo p de $\mathrm{Res}(Q_m,Q_n)$ est non nulle pour tout p premier. Ce qui entraîne bien que $\mathrm{Res}(Q_m,Q_n)$ est un inversible de $\mathbb{Z}$.

Démontrons le théorème dans le cas particulier ou n est un nombre premier p. Rappelons que, modulo p, $X^p-1=(X-1)^p$. Donc la réduction modulo p de $H_p(X)$ est $(X-1)^{p-1} = [(X-1)^2]^{\frac{p-1}{2}} = (X^2-2X+1)^{\frac{p-1}{2}} = X^{\frac{p-1}{2}}\cdot\left(X+\frac{1}{X}-2\right)^{\frac{p-1}{2}}$.

Ceci montre que la réduction modulo p de $Q_p(Y)$ est $\overline{Q_p}(Y)=(Y-2)^{\frac{p-1}{2}}$.

La réduction modulo p de $Res(Q_p,Q_m)$ est :

$$\overline{Res}\left(\overline{Q_p}, \overline{Q_m}\right) = (Res(Y-2, \overline{Q_m})^{\frac{p-1}{2}} = \left[\overline{Q_m}(2)\right]^{\frac{p-1}{2}}.$$

Mais $Q_m(2) = Q_m\left(1+\frac{1}{1}\right) = 1.H_m(1) = m$. On obtient que $Res(Q_p,Q_m)\equiv m^{\frac{p-1}{2}}[p]$. Mais on sait déjà que $Res(Q_p,Q_m)=\pm 1$ et grâce au lemme d'Euler (voir en III.), on constate bien que le théorème est prouvé dans ce cas.

On ne traitera pas le cas général. La preuve est élémentaire mais sans intérêt particulier pour notre propos.

On peut facilement décrire les racines de Q_n. Il s'agit des $\frac{n-1}{2}$ réels $z+\frac{1}{z}$, ou z est une racine $n^{ième}$ complexe de l'unité – autre que 1. Autrement dit il s'agit des $\frac{n-1}{2}$ nombres $2\cos\frac{2\pi s}{n}\left(s=1, \ldots, \frac{n-1}{2}\right)$.

En particulier,

Corollaire (G. Eisenstein)

$$\binom{n}{m} = (2)^{\frac{m-1}{2}\frac{n-1}{2}} \prod_{s=1}^{\frac{n-1}{2}} \prod_{t=1}^{\frac{m-1}{2}} \left(\cos\frac{2\pi t}{m} - \cos\frac{2\pi s}{n}\right)$$

On peut donner une jolie interprétation géométrique à ce résultat. Remarquons que si $z = e^{\frac{2i\pi s}{n}}$, $(1-z)(\overline{1-z}) = 2-(z+\overline{z})$. Ainsi $2-2\cos\frac{2\pi s}{n}$ représente le carré de la longueur du segment joignant les points du plan complexe d'affixes 1 et $z = e^{\frac{2i\pi s}{n}}$.

Puisque $2\left(\cos\frac{2\pi t}{m} - \cos\frac{2\pi s}{n}\right) = \left(2-2\cos\frac{2\pi s}{n}\right) - \left(2-2\cos\frac{2\pi t}{m}\right)$ (sic!), on vient de prouver le résultat suivant, annoncé dans l'introduction.

Théorème : Soit b un entier impair positif, supérieur ou égal à 3.

Notons $\ell_1^2(b)$, ..., $\ell_{\frac{b-1}{2}}^2(b)$, les différents carrés des longueurs des polygones réguliers à b côtés, étoilés ou pas, convexes ou pas, mais inscrits dans un cercle de rayon 1. Alors,

$$\binom{n}{m} = \prod_{s=1}^{\frac{n-1}{2}} \prod_{t=1}^{\frac{m-1}{2}} (\ell_s^2(n) - \ell_t^2(m))$$

L'étude des polygones réguliers préoccupe les mathématiciens, et d'autres, depuis toujours. Le *"calcul"* des longueurs des côtés de ces polygones est très ancien, bien antérieur à toute découverte des nombres complexes. On trouve dès le 16ème siècle la détermination, pour de petites valeurs de n, du polynôme K_n dont les zéros sont les carrés de ces longueurs. On a vu que $K_n(Y)=Q_n(2-Y)$ et il suit que $\binom{n}{m} = \text{Res}(K_n,K_m)$. Le calcul de K_7 est par exemple donné dans la grande œuvre de J. Kepler (Harmonices Mundi, Linz, 1619, voir pages 32 à 37 dans la traduction française de J. Peyroux éditée par A. Blanchard, 1979). Il attribue d'ailleurs ce calcul à un autre mathématicien : Justus Byrgius (ou Joost Bürgi), suisse né à Lichtensteig (1549) et mort à Cassel (1632).

La méthode, connue dès l'antiquité, de construction du pentagone régulier avec la règle et le compas peut d'ailleurs s'interpréter comme un *"calcul"* de $K_5(Y)=Y^2-5Y+5$. Ces polynômes K_n sont parmi les plus anciens polynômes remarquables.

Références.

Bachmann P. : Niedere Zahlentheorie, Erster Teil, B.G. Teubner, Leipzig 1902.

Cartier P. : Sur une généralisation des symboles de Legendre–Jacobi, L'enseignement mathématique, 16, (1970), p.31–48.

Eisenstein G. : Application de l'Algèbre à l'Arithmétique transcendante, Journal de Crelle 29 (1845), p.177–184, reproduit dans : Mathematische Werke I, p.291–298, Chelsea pub. (1989).

Kronecker L. : Verallgemeinerung des Gaußschen Kriteriums für den quadratischen Restcharakter einer Zahl in bezug auf eine andere, Monatsber. K. Akad. Win. zu Berlin, Sitzung v.22 Juni 1876, (1878), p.330–341.

Pieper, H : Variationen über ein zahlentheoretisches Thema von C.F. Gauss, Birkhäuser V. Basel und Stuttgart, 1978.

Zolotareff E.I. : Nouvelle démonstration de la loi de réciprocité de Legendre, Nouv. Ann. Math. (2) 11 (1872), p.354–362.