LEÇON 102

GROUPE DES NOMBRES COMPLEXES DE MODULE 1. SOUS-GROUPES DES RACINES DE L'UNITÉ. APPLICATIONS.

Motivation Le cercle unité et les sous-groupes des racines de l'unité interviennent naturellement dans divers domaines de l'algèbre. On peut citer l'algèbre linéaire où les valeurs propres de matrices de groupes remarquables sont dans le cercle unité ou sont des sous-groupes des racines de l'unité. Nous en profitons pour faire une longue étude sur l'exponentielle complexe, la définition du nombre 2π et les angles. On peut aussi étudier les caractères des groupes abéliens, ce qui nous sert à démontre le résultat très intuitif de structure des groupes abéliens finis. On peut encore citer les polynômes cyclotomiques et leurs applications à la théorie des corps, comme le théorème de Wedderburn ou encore le fait que tout sur-corps de $\mathbf{Q}$ de dimension finie admet un nombre fini de racines de l'unité (application 7 à la page 51).

Attendus du jury et choix à faire Parmi les incontournables de la leçon :

- ne pas se pas se cantonner aux aspects élémentaires ;
- ne pas oublier la partie groupe de la leçon ;
- donner des domaines en algèbre où les complexes de module 1 apparaissent.

Parmi les plus :

- l'exponentielle complexe et ses applications ;
- polynômes cyclotomiques ;
- spectre de matrices remarquables ;
- théorie des représentations ;
- relèvement du groupe unité au groupe additif des réels (à l'aide de ϕ^{-1}) ;
- $\mathbf{Q}[\mathrm{i}]$ et ses racines de l'unité ;

— sous-groupes compacts de $\mathbf{C}^*$;
— transformée de Fourier discrète et rapide.

Développements

— Définition du nombre 2π, chapitre 266 à la page 531 ;
— Théorème de Wedderburn [Per98] ;
— Caractérisation de n dans $\mathrm{GL}_n(\mathbf{K})$, chapitre 267 à la page 535 ;
— Développements sur les caractères ou les représentations ;
— L'application 7 ;
— Vous trouverez dans [PI19] plusieurs développements possible : des résultats sur les polynômes cyclotomiques (irréductibilité, théorème de Kronecker et l'application), la transformée de Fourier discrète et le théorème de structure des groupes abéliens finis.

Références [Per98], [Pey04], [Vid01].

I Généralités sur $\mathbf{U}$ et $\mathbf{U}_n$; bases de trigonométrie

I.1 Définitions et premiers résultats

Définition 1. — On note $\mathbf{U}$ l'ensemble des $z \in \mathbf{C}$ tels que $|z| = 1$.
— Soit $n \in \mathbf{N}^*$, on note $\mathbf{U}_n$ l'ensemble des $z \in \mathbf{C}$ tels que $z^n = 1$.

Remarque orale. On ne sait toujours pas ici que les solutions de $X^n - 1$ sont les $\mathrm{e}^{\frac{2ik\pi}{n}}$. On va définir le nombre 2π plus tard.

Proposition I.1. Le cardinal de $\mathbf{U}_n$ est n (conséquence du théorème de D'Alembert-Gauss).

Théorème I.2. $\mathbf{U} < \mathbf{C}^*$ et les $\mathbf{U}_n$ sont des sous-groupes de $\mathbf{U}$.

Proposition I.3. Soit $H < \mathbf{C}^*$ borné alors $H < \mathbf{U}$.

Théorème I.4. Soit $H < \mathbf{C}^*$ un sous-groupe fini, alors H est cyclique.

Application 1. $\mathbf{U}_n$ est cyclique.

I.2 L'exponentielle complexe

Remarque orale. Cette sous-partie est là pour mieux comprendre le cercle unité et sert surtout à exhiber les racines n^{e} de l'unité.

Définition 2. — $\exp : \mathbf{C} \to \mathbf{C}$ qui à z associe $\sum_{n=0}^{+\infty} \frac{z^n}{n!}$ qui est bien définie ;
— On note ϕ la fonction de $\mathbf{R}$ dans $\mathbf{C}$, qui à t associe $\exp(\mathrm{i}t)$ [1].

1. On peut montrer la non injectivité de exp en passant par un argument de simple connexité et définir ϕ juste après la proposition I.7.

Proposition I.5 (Premières propriétés)**.** 1. $\forall z, z' \in \mathbf{C} : \exp(z+z') = \exp(z)\exp(z')$.

2. $\exp$ est holomorphe, et est égale à sa propre dérivée.
3. $\exp$ ne s'annule jamais ; elle est localement ouverte (théorème inversion locale), $\exp$ est donc une application ouverte.

Théorème I.6. $\exp$ réalise un morphisme de groupe de $(\mathbf{C}, +)$ dans $(\mathbf{C}^*, \times)$, surjectif $(\exp(\mathbf{C}) = \mathbf{C}^*)$ mais non injectif. De même, ϕ réalise un morphisme de groupe de $(\mathbf{R}, +)$ dans $(\mathbf{U}, \times)$, surjectif mais non injectif.

Proposition I.7 (Étude de $\operatorname{Ker}\exp = \mathrm{i}\operatorname{Ker}\phi$)**.** $\operatorname{Ker}\phi$ est un sous-groupe non trivial de $\mathbf{R}$, fermé. Il est donc de la forme $b\mathbf{Z}$, où $b = \inf\{x > 0, \phi(x) = 0\}$. En particulier, $b \neq 0$.

Définition 3. On définit le nombre $\tau = 2\pi$ tel que $\operatorname{Ker}\phi = 2\pi\mathbf{Z}$.

Corollaire. $\mathbf{U}$ est isomorphe à $\mathbf{R}/2\pi\mathbf{Z}$.

Application 2. Les éléments de $\mathbf{U}_n$ sont les $\omega_k := \exp\left(\mathrm{i}\frac{2\pi k}{n}\right)$ pour $k \in \{0; 1; 2; \ldots; n-1\}$.

Définition 4. On rappelle que $\mathbf{U}_n$ est cyclique. Une racine n^{e} de l'unité est dite primitive si elle engendre $\mathbf{U}_n$.

Proposition I.8. ω_k défini précédemment est racine primitive ssi k est premier à n.

I.3 Angles et rotations planes [Vid01]

On rappelle : $\mathrm{SO}(2) = \{\phi \in \mathrm{O}(2) : \det(\phi) = 1\}$. On note E le plan vectoriel de $\mathbf{R}^2$ muni du produit scalaire usuel. La sphère unité de E est notée $\mathcal{S}^1$.

On rappelle que $\mathbf{U} = \{u \in \mathbf{C} : |u| = 1\}$. On identifie le plan complexe à $\mathbf{R}^2$, donc $\mathbf{U}$ est confondu avec la sphère unité $\mathcal{S}^1$ de $\mathbf{R}^2$.

Théorème I.9. $\mathrm{SO}(2)$ agit transitivement et simplement sur $\mathbf{U}$, c'est-à-dire :
$\forall u, v \in \mathbf{U},\ \exists!\ f \in \mathrm{SO}(2)$ tel que $f(u) = v$.

Démonstration. $\mathrm{SO}(2)$ agit transitivement : notons τ la symétrie d'axe $D = \mathbf{R}(u+v)$ et τ' la symétrie d'axe $\mathbf{R}v$. Alors $\tau' \circ \tau \in \mathrm{SO}(2)$ et $\tau' \circ \tau(u) = v$.

$\mathrm{SO}(2)$ agit simplement : supposons qu'il existe f et g telles que $f(u) = g(u)$. Alors l'application $g^{-1} \circ f \in \mathrm{SO}(2)$ fixe point par point la droite $\mathbf{R}u$, donc $g^{-1} \circ f = id$.

(On utilise le fait que si $f \in \mathrm{SO}(2)$ fixe une droite D point par point, alors $f = id$.) □

Définition 5. L'espace E est dit orienté lorsque l'on a choisi une base orthonormée de référence $\beta = (e_1, e_2)$. Une base orthonormée $\beta' = (e'_1, e'_2)$ de E est dite orientée dans le sens direct lorsqu'il existe $f \in \mathrm{SO}(2)$ telle que $f(e_i) = e'_i$ pour $i = 1, 2$. Autrement dit, lorsque $\det f = \det_\beta \beta' = 1$. Plus généralement, une base quelconque β'' est dite directe ou orientée dans le même sens que β lorsque $\det_\beta \beta'' > 0$.

À partir de là, on fixe une base $\mathcal{B} = (e_1, e_2)$ orthonormée de E, et on note $\mathrm{Mat}_{\mathcal{B}}(f)$ la matrice associée à $f \in \mathrm{O}(2)$ dans cette base.

Définition 6. On définit $\sin(\theta) := \mathrm{Im}(\phi(\theta))$ et $\cos(\theta) = \mathrm{Re}(\phi(\theta)))$. On a donc les formules classiques : $\exp(\mathrm{i}x) = \cos(x) + \mathrm{i}\sin(x)$, $\cos(x) = \dfrac{\exp(\mathrm{i}x) + \exp(-\mathrm{i}x)}{2}$ et $\sin(x) = \dfrac{\exp(\mathrm{i}x) - \exp(-\mathrm{i}x)}{2\,\mathrm{i}}$. De plus, cos et sin sont 2π-périodiques.

Proposition I.10. $\rho : \left| \begin{array}{ccc} \mathbf{U} & \to & \mathrm{SO}_2(\mathbf{R}) = \{\mathrm{Mat}(f) : f \in \mathrm{SO}(2)\} \\ \exp(\mathrm{i}\theta) & \mapsto & R(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \end{array} \right.$
est un isomorphisme topologique de groupes.
En particulier, $\mathrm{SO}_2(\mathbf{R})$ est commutatif, connexe et compact.

Remarque pour le lecteur. On peut aussi écrire ρ comme : $\left| \begin{array}{ccc} \mathbf{U} & \to & \mathrm{SO}_2(\mathbf{R}) \\ a + \mathrm{i}b & \mapsto & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{array} \right.$

I.4 Angles orientés de vecteurs

Soit $\mathcal{A}$ l'ensemble des couples de vecteurs unitaires de $\mathbf{R}^2$. On définit sur $\mathcal{A}$ la relation d'équivalence : $(u, v) \sim (u', v') \iff \exists R_\theta \in \mathrm{SO}_2(\mathbf{R})$ tel que $R_\theta(u) = u'$ et $R_\theta(v) = v'$.

Définition 7. $\mathcal{A}/_\sim$ est l'ensemble des angles orientés de vecteurs.

Proposition I.11. L'application de $\mathcal{A}/_\sim$ dans $\mathrm{SO}_2(\mathbf{R})$ qui à un représentant (u, v) associe $R_\theta \in \mathrm{SO}_2(\mathbf{R})$ tel que $R_\theta(u) = v$ est bien définie et est une bijection.

Proposition I.12 (Relation de Chasles)**.** $\forall u, v, w \in \mathcal{S}^1, (u, v) + (v, w) = (u, w)$.

Démonstration. Notons f (respectivement g) la rotation correspondante à (u, v) (resp. à (v, w)). Alors $f(u) = v$ et $g(v) = w$, donc $g \circ f(u) = v$. □

Proposition I.13. L'isomorphisme $\mathbf{R}/_{2\pi\mathbf{Z}} \to \mathrm{SO}_2(\mathbf{R})$ permet de définir une mesure des angles orientés de vecteurs.

Démonstration. $\mathcal{A} \simeq \mathrm{SO}(2) \simeq \mathrm{SO}_2(\mathbf{R}) \simeq \mathbf{U} \simeq \mathbf{R}/_{2\pi\mathbf{Z}}$. □

L'isomorphisme entre $\mathrm{SO}(2)$ et $\mathrm{SO}(2, \mathbf{R})$ dépend de l'orientation de E, c'est-à-dire du choix d'une base orthonormée de référence. Comme $\left| \begin{array}{ccc} \mathbf{R} & \to & \mathbf{U} \\ \theta & \mapsto & \exp(\mathrm{i}\theta) \end{array} \right.$ est un morphisme de groupe surjectif dont le noyau est $2\pi\mathbf{Z}$; on a l'isomorphisme :

$\left| \begin{array}{ccc} \mathbf{R}/_{2\pi\mathbf{Z}} & \to & \mathbf{U} \\ \theta & \mapsto & \exp(\mathrm{i}\theta) \end{array} \right.$ A chaque angle correspond donc un nombre réel défini à 2π près. Ce nombre s'appelle la mesure de cet angle.

Dans la pratique, dès que l'on a défini une orientation sur E, alors $\mathcal{A}/_\sim$, $\mathrm{SO}(2)$ et $\mathbf{R}/_{2\pi\mathbf{Z}}$ deviennent des ensembles indiscernables en tant que groupes. On parle alors indifféremment d'une rotation, d'un angle ou de sa mesure.

II Étude approfondie de $\mathbf{U}_n$ et de $\mathbf{U}$

II.1 Sous-groupes de $\mathrm{GL}_n(\mathbf{C})$ et $\mathbf{U}$

Proposition II.1. Soit $G < \mathrm{GL}_n(\mathbf{C})$ d'exposant fini, noté exp(G), alors pour $g \in G$, on a $\mathrm{Sp}(g) \subset \mathbf{U}_{\exp(G)}$, où $\exp(G)$ est l'exposant de G (et pas l'exponentielle).

Théorème II.2 (Caractérisation de n dans $\mathrm{GL}_n(\mathbf{R})$)**.** $\mathrm{GL}_n(\mathbf{R}) \approx \mathrm{GL}_m(\mathbf{R})$ ssi $n = m$.

Remarque pour le lecteur. Utilise la diagonalisation simultanée d'une famille d'endomorphisme diagonalisables qui commutent deux à deux.

Proposition II.3. Soit $G < \mathrm{GL}_n(\mathbf{C})$ compact. Les valeurs propres de $g \in G$ sont dans $\mathbf{U}$.

Application 3. Soit $g \in \mathrm{O}_n(\mathbf{R})$, alors les valeurs propres de g sont dans $\mathbf{U}$.

II.2 Matrices circulantes

Définition 8. Soit $(c_0, c_1, \ldots, c_N) \in \mathbf{C}^N$. On définit la matrice circulante $C(c_0, c_1, \ldots, c_N)$ par : $\begin{pmatrix} c_0 & c_{n-1} & \ldots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & & c_2 \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ & & \ddots & \ddots & c_{n-1} \\ c_{n-2} & & & & \\ c_{n-1} & c_{n-2} & \ldots & c_1 & c_0 \end{pmatrix}$, que l'on notera par commodité C.

On appelle $P_C(X) := c_0 + c_1 X + \ldots c_{n-1} X^{n-1}$ le polynôme associée à la matrice C.

Proposition II.4. La famille des vecteurs $v_j = \dfrac{1}{\sqrt{n}}\omega_j$ forme une base orthonormale de vecteurs propres, associés aux valeurs propres $\lambda_j = P_C(w_j)$ où $\omega_j = \exp(\mathrm{i}\frac{2\pi j}{n})$.

Proposition II.5. $\det C = \prod_{j=0}^{n-1} P_C(w_j)$.

II.3 Transformée de Fourier rapide (FFT) [Pey04] et [Dem09]

Se référer à la leçon 107 sous-section III.3 à la page 79 .

III Dual d'un groupe abélien fini [Pey04]

Dans toute cette section on note G un groupe abélien fini de cardinal $n \in \mathbf{N}^*$.

III.1 Définitions

Définition 9.
— χ est un caractère de G si $\chi : G \to \mathbf{C}^*$ est un morphisme de groupes.
— On note $\widehat{G}$ l'ensemble des caractères de G. $\widehat{G}$ est appelé le dual de G.

Théorème III.1. $\widehat{G}$ est un groupe abélien pour la multiplication classique des applications.

III.2 Dual d'un groupe cyclique

Proposition III.2 (Fondamentale)**.** Soit $G := \{1, g_0, g_0^2, \dots, g_0^{n-1}\}$ un groupe cyclique de générateur g_0. Soit ω une racine primitive n^e de l'unité, par exemple $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$. Alors les éléments de $\widehat{G}$ sont de la forme $\chi_j : G \to \mathbf{C}^*; g = g_0^k \mapsto (\omega^j)^k$, pour $j \in \{0, \dots, n-1\}$.

Application 4 (Table de $\mathbf{Z}/n\mathbf{Z}$)**.** Leçon 107, application 9 à la page 79 .

Application 5. Si G est cyclique, alors $\widehat{G} \approx G$. Ainsi, il existe $\chi \in \widehat{G}$ bijective sur $\mathbf{U}_n$.

III.3 Structure des groupes abéliens finis.

Lemme III.3 (Prolongement des caractères)**.** Soit $H < G$. Tout caractère χ de H peut être prolongé en un caractère de G. De plus, il y a exactement $[G : H]$ manières de le faire [Ell75].

Remarque. En fait le théorème de prolongement des caractères (partie existence) nous dit que si l'on a $H < G$ et un morphisme de H qui arrive dans un corps algébriquement clos et tel que pour tout $g \in G \; \exists \; r \in \mathbf{N}^*$ tel que $g^r \in H$, alors nous pouvons prolonger le morphisme à tout le groupe. C'est sans doute le meilleur parallèle avec le prolongement des applications uniformément continues.

Théorème III.4 (Structure des groupes abéliens finis [Ell75])**.** Il existe $(p_i, \alpha_i, \beta_i) \in (\mathcal{P} \times \mathbf{N}^* \times \mathbf{N}^*)^r$ tels que $G \approx \prod_{i=1}^{r} \left(\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}\right)^{\beta_i}$ où $\mathcal{P}$ est l'ensemble des nombres premiers positifs.

De plus cette écriture est unique si $(i \neq j \text{ et } p_i = p_j) \implies (\alpha_i \neq \alpha_j)$.

Remarque pour le lecteur. En général la décomposition en produit de cycles n'est pas écrite ainsi mais plutôt avec des entiers qui se divisent les uns les autres. Nous avons juste utilisé le lemme chinois pour arriver à une telle décomposition.

Corollaire. $G \approx \widehat{G}$ (procéder par récurrence sur le cardinal de G).

IV Polynômes cyclotomiques [Per98]

IV.1 $\Phi_n \in \mathbf{Z}[X]$

Définition 10. Le n^e polynôme cyclotomique noté $\Phi_n(X) \in \mathbf{C}[X]$ est donné par la formule : $\Phi_n(X) := \prod_{\zeta \in \mathbf{U}_n^{\text{gen}}} (X - \zeta)$ où $\mathbf{U}_n^{\text{gen}}$ est l'ensemble des racines n^e primitives de l'unité.

Proposition IV.1. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Application 6 (Calcul des polynômes cyclotomiques)**.** On a $\Phi_1(X) = X - 1$. Puis :

- $X^2 - 1 = \Phi_2\Phi_1$ donc $\Phi_2 = X + 1$;
- $X^3 - 1 = \Phi_3\Phi_1$ donc $\Phi_3 = X^2 + X + 1$;
- $X^4 - 1 = \Phi_4\Phi_2\Phi_1$ donc $\Phi_4 = X^2 + 1$;

— pour p premier, on a $X^p - 1 = \Phi_p \Phi_1$, donc $\Phi_p = X^{p-1} + X^{p-2} + \cdots + 1$.

Remarque pour le lecteur. Il y a 100% de chances que le jury vous demande de calculer les premiers polynômes cyclotomiques. Éviter de passer par la formule avec les exponentielles complexes et de croire que vous allez y arriver, sous peine de rentrer dans le bêtisier.

Remarque pour le lecteur. Ne pas croire que les coefficients des polynômes cyclotomiques valent toujours ± 1 ou 0; on peut avoir d'autres coefficients, même s'il faut aller chercher assez loin (le premier candidat est $3 \times 5 \times 7 = 105$, et il s'avère que ϕ_{105} possède un coefficient qui vaut -2).

Corollaire. $n = \sum_{d|n} \phi(d)$ où ϕ est l'indicatrice d'Euler.

Théorème IV.2. Soit $n \in \mathbf{N}^*$ alors $\Phi_n(X) \in \mathbf{Z}[X]$.

IV.2 Applications

Théorème IV.3 (Wedderburn)**.** Tout anneau fini sans diviseurs de 0 est un corps.

Démonstration. Soit A un anneau fini sans diviseurs de 0. Montrons que tout élément non nul de A admet un inverse puis le reste de la démonstration est dans [Per98].
Soit $x \in A \backslash \{0\}$. Considérons $f_x : A \to A$ qui à y associe xy alors f_x est une application injective. Par cardinalité elle est aussi surjective, ainsi 1 est atteint. □

Théorème IV.4. Le polynôme cyclotomique $\Phi_n(X)$ est irréductible dans $\mathbf{Z}[X]$.

Remarque pour le lecteur. C'est un développement possible, sinon vous pouvez admettre le théorème. Il est plus facile de montrer que les $\Phi_{p^m}(X)$ sont irréductibles (cf. leçon 125).

Application 7. Soit $n \in \mathbf{N}^*$. Alors il existe $m \in \mathbf{N}$ tel que si $\mathbf{Q} \subset \mathbf{K} \subset \mathbf{C}$ et $[\mathbf{K} : \mathbf{Q}] = n$, alors $\mathbf{K}^* \cap \mathbf{U} \subset \mathbf{U}_m$.

Démonstration. Remarquons que si $n = p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$, alors $\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$. En ordonnant les p_i, on peut facilement montrer par récurrence que $p_i \geq i + 1$. Ainsi $\phi(n) \geq n \prod_{i=1}^{r} \left(1 - \frac{1}{i+1}\right) = n \prod_{i=1}^{r} \left(\frac{i}{i+1}\right) = n \times \frac{1}{r}$. Comme $r \leq \log_2(n)$ (car 2 est le plus petit des nombres premiers !), on obtient $n \times \frac{1}{r} \geq \frac{n}{\log_2(n)}$ qui tend vers l'infini quand n tend vers plus l'infini.
Soit $r \in \mathbf{N}$ tel que si $M > r$ alors $\phi(M) > n$.
Remarquons que toutes les racines de l'unité sont des racines primitives l^{e} de l'unité pour un certain l. Donc nous pouvons ne considérer que les racines primitives de l'unité.
Supposons par l'absurde qu'il existe une racine M^{e} primitive de l'unité dans $\mathbf{K}$. Notons ζ_M une racine M^{e} primitive de l'unité. On a $\mathbf{Q}(\zeta_M) \subset \mathbf{K}$ et $[\mathbf{Q}(\zeta_M) : \mathbf{Q}] = \phi(M) > n$ par le théorème IV.4, ce qui est absurde par multiplicativité des degrés. Ainsi $\mathbf{K}$ ne contient que des racines primitives au maximum r^{e} de l'unité.
Notons G le groupe engendré par $\bigcup_{i=1}^{r} \mathbf{U}_i$. On montre facilement par récurrence que

$G = \mathbf{U}_{\mathrm{ppcm}\{1;..;r\}}$ (il suffit de le faire pour $< \mathbf{U}_n; \mathbf{U}_m >$). Toutes les racines de l'unité de $\mathbf{K}$ sont incluses dans $\bigcup_{i=1}^{r} \mathbf{U}_i$, donc dans $G = \mathbf{U}_{\mathrm{ppcm}\{1;..;r\}}$. □