Leçon 102. Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

1. Les nombres complexes de module 1

1.1. Structure de groupe

1. Proposition. L'application
$$\left|\begin{array}{l}\mathbf{C}\longrightarrow\mathbf{R}_+^*,\\ z\longmapsto|z|\end{array}\right.$$
est un morphisme de groupes multiplicatif. Son noyau $\mathbf{U}\subset\mathbf{C}$ est le *groupe des nombres complexes de module 1.*

2. Exemple. Les nombres ±1 et $\pm i$ appartiennent au groupe $\mathbf{U}$.

3. Remarque. On note $\mathbf{S}^1\subset\mathbf{R}^2$ la sphère unité euclidienne de $\mathbf{R}^2$. Alors l'application
$$\left|\begin{array}{l}\mathbf{U}\longrightarrow\mathbf{S}^1,\\ a+ib\longmapsto(a,b)\end{array}\right.$$
est un homéomorphisme.

4. Proposition. L'application
$$\left|\begin{array}{l}\mathbf{R}_+^*\times\mathbf{U}\longrightarrow\mathbf{C}^*,\\ (r,u)\longmapsto ru\end{array}\right.$$
est un isomorphisme de groupes.

5. Proposition. Le groupe $\mathbf{U}$ est compact et connexe par arcs.

1.2. Fonctions exponentielle et trigonométriques

6. Définition. L'*exponentielle* d'un nombre complexe $z\in\mathbf{C}$ est le nombre
$$\exp z\coloneqq\sum_{n=0}^{+\infty}\frac{z^n}{n!}.$$
On le note aussi e^z.

7. Proposition. La fonction $\exp\colon\mathbf{C}\longrightarrow\mathbf{C}^*$ est un morphisme de groupes surjectif. De plus, elle est holomorphe.

8. Lemme. Un sous-groupe additif du groupe $\mathbf{R}$ est soit dense soit de la forme $a\mathbf{Z}$ pour un réel $a\in\mathbf{R}$.

9. Proposition. L'application
$$\left|\begin{array}{l}\mathbf{R}\longrightarrow\mathbf{U},\\ t\longmapsto e^{it}\end{array}\right.$$
est bien définie et il s'agit d'un morphisme surjectif entre les groupes $(\mathbf{R},+)$ et $(\mathbf{U},\times)$ de noyau $a\mathbf{Z}$ pour un réel $a>0$. On note $\pi\coloneqq a/2$ En particulier, il induit un isomorphisme de groupes
$$\mathbf{U}\simeq\mathbf{R}/2\pi\mathbf{Z}.$$

10. Corollaire. L'application
$$\left|\begin{array}{l}\mathbf{R}_+^*\times[0,2\pi[\longrightarrow\mathbf{C}^*,\\ (r,t)\longmapsto re^{it}\end{array}\right.$$
est bijective.

11. Définition. Pour un réel $t\in\mathbf{R}$, on définit son *cosinus* et son *sinus* comme les nombres réels
$$\cos t\coloneqq\operatorname{Re}e^{it}\qquad\text{et}\qquad\sin t\coloneqq\operatorname{Im}e^{it}.$$

12. Proposition. Soit $t\in\mathbf{R}$ un réel.
- Les fonctions cos et sin sont dérivables et $\sin' t=\cos t$ et $\cos' t=\sin t$.
- Elles sont 2π-périodiques.
- On a $\cos^2 t+\sin^2 t=1$.

1.3. Mesure d'un angle orienté

13. Définition. Un *argument* d'un nombre complexe $z\in\mathbf{C}$ est un réel $\theta\in\mathbf{R}$ tel que $z=|z|\,e^{i\theta}$.

14. Proposition. Toute matrice $A\in\mathrm{SO}(2)$ est de la forme
$$A=\begin{pmatrix}a&-b\\ b&a\end{pmatrix}\quad\text{avec}\quad a,b\in\mathbf{R},\ a^2+b^2=1,$$
c'est-à-dire qu'il existe un réel $\theta\in\mathbf{R}$ tels que
$$A=R(\theta)\coloneqq\begin{pmatrix}\cos\theta&-\sin\theta\\ \sin\theta&\cos\theta\end{pmatrix}.$$
Autrement, le groupe $\mathrm{SO}(2)$ est isomorphe au groupe $\mathbf{U}$.

15. Définition *(notion d'angle dans un plan).* Soient $u,v\in\mathbf{U}$ deux nombres complexes unitaires vus comme des points du $\mathbf{R}$-espace vectoriel $\mathbf{C}\simeq\mathbf{R}^2$. Alors il existe un et une seule isométrie $f\in\mathrm{O}(\mathbf{R}^2)$ telle que $f(u)=v$. Un réel $\theta\in\mathbf{R}$ tel que la matrice $R(\theta)$ représente l'isométrie f est une *mesure de l'angle* du couple (u,v).

16. Proposition. Soit $z\in\mathbf{C}$ un nombre complexe qu'on note sous la forme $z=|z|\,e^{i\theta}$. Alors le réel θ est une mesure de l'angle du couple $(0,e^{i\theta})$.

2. Racines de l'unité et cyclotomie

2.1. Racines de l'unité

17. Définition. Soit $n\geqslant1$ un entier non nul. Une *racine n-ième de l'unité* est un nombre complexe $\zeta\in\mathbf{C}$ tel que $\zeta^n=1$. On note $\mathbf{U}_n$ l'ensemble des racines n-ièmes de l'unité.

18. Exemple. Le nombre complexe $e^{2i\pi/n}$ est une racine n-ième de l'unité.

19. Proposition. L'ensemble $\mathbf{U}_n$ est un sous-groupe de $\mathbf{U}$ d'ordre n.

20. Définition. Une racine $\zeta\in\mathbf{U}_n$ est *primitive* si elle engendre le groupe $\mathbf{U}_n$. On note $\mathbf{U}_n^\times$ l'ensemble des racines n-ièmes primitives de l'unité.

21. Proposition. L'ensemble $\mathbf{U}_n^\times$ est un sous-groupe de $\mathbf{U}$ d'ordre $\varphi(n)$.

22. Proposition. On a $\mathbf{U}_n=\bigsqcup_{d|n}\mathbf{U}_d$.

2.2. Les polynômes cyclotomiques et leurs applications

23. Définition. Le *n-ième polynôme cyclotomique* est le polynôme

$$\Phi_n \coloneqq \prod_{\zeta \in \mathbf{U}_n^\times} (X - \zeta) \in \mathbf{C}[X].$$

24. Proposition. On a

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

25. Exemple. On a $\Phi_1 = X - 1$, puis $\Phi_2 = X + 1$ et $\Phi_3 = X^2 + X + 1$.

26. Application *(théorème de Weddenburn).* Tout corps fini est commutatif.

27. Corollaire. Le polynôme Φ_n est à coefficients entiers et de degré $\varphi(n)$.

28. Théorème. Le polynôme Φ_n est irréductible sur $\mathbf{Q}$ et sur $\mathbf{Z}$.

29. Corollaire. Soit $\zeta \in \mathbf{U}_n^\times$. Alors $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n)$.

3. Applications à l'algèbre

3.1. Matrices circulantes et valeurs propres

30. Définition. Une *matrice circulante* est une matrice de la forme

$$C(a_1, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix} \in \mathscr{M}_n(\mathbf{C})$$

pour des complexes $a_1, \dots, a_n \in \mathbf{C}$.

31. Proposition. Soient $a_1, \dots, a_n \in \mathbf{C}$ des complexes. On pose $\omega \coloneqq e^{2i\pi/n}$ et

$$P \coloneqq a_1 + a_2 X + \cdots + a_n X^{n-1} \in \mathbf{C}[X].$$

Alors

$$\det C(a_1, \dots, a_n) = P(1)P(\omega) \cdots P(\omega^{n-1}).$$

32. Corollaire. Le spectre complexe de la matrice $C(a_1, \dots, a_n)$ est constitué des nombres $P(1)$, …, $P(\omega^{n-1})$.

33. Proposition. Soit $(P^k)_{k \in \mathbf{N}}$ une suite de $\mathbf{C}^n$ qu'en notant $P^k = (z_1^k, \dots, z_n^k)$ pour tout entier $k \in \mathbf{N}$, elle satisfasse la relation

$$P^{k+1} = \left(\frac{z_1^k + z_2^k}{2}, \frac{z_2^k + z_3^k}{2}, \dots, \frac{z_n^k + z_1^k}{2} \right), \qquad k \in \mathbf{N}.$$

Alors la suite $(P^k)_{k \in \mathbf{N}}$ converge vers l'élément $(g, \dots, g) \in \mathbf{C}^n$ avec

$$g \coloneqq \frac{z_1^0 + \cdots + z_n^0}{n}.$$

3.2. La transformée de Fourier discrète

34. Définition. La *transformée de Fourier discrète* est l'application

$$\mathrm{DFT}_n : \left| \begin{array}{l} \mathbf{C}[X] \longrightarrow \mathbf{C}^n, \\ \quad F \longmapsto (F(1), \dots, F(\omega^{n-1})) \end{array} \right.$$

avec $\omega \coloneqq e^{2i\pi/n}$.

35. Proposition. L'application $\mathrm{DFT}_n : \mathbf{C}[X]/(X^n - 1) \longrightarrow \mathbf{C}^n$ est un isomorphisme de $\mathbf{C}$-algèbres.

36. Remarque *(algorithme).* On souhaite multiplier deux polynômes $F, G \in \mathbf{C}[X]_{<n}$. On procède en trois étapes :

- on calcul efficacement les n-uplets $\mathrm{DFT}_n(F)$ et $\mathrm{DFT}_n(G)$ (cf. ci-dessous) ;
- on fait le produit terme à terme de ces derniers, on obtient le n-uplet $\mathrm{DFT}_n(FG)$;
- on interpole.

37. Proposition. On suppose que $n = 2k$ avec $k \in \mathbf{N}^*$. Soit $F \in \mathbf{C}[X]_{<n}$ un polynôme. On écrit des divisions euclidiennes

$$F = (X^k - 1)F_0 + R_0 \qquad \text{et} \qquad F = (X^k + 1)F_1 + R_1.$$

Soit $\ell \in [\![0, n-1]\!]$. Alors

- si l'entier ℓ est pair, alors $F(\omega^\ell) = R_0(\omega^\ell)$.
- si l'entier ℓ est impair, alors $F(\omega^\ell) = R_1(\omega^\ell)$.

38. Théorème. L'algorithme prend au plus $\frac{3n}{2} \log n$ opérations sur le corps $\mathbf{C}$.

[1] Michèle Audin. *Géométrie.* EDP Sciences, 2006.
[2] Alin Bostan et al. *Algorithmes Efficaces en Calcul Formel.* 2017.
[3] Xavier Gourdon. *Analyse.* 2e édition. Ellipses, 2008.
[4] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.