Chapitre 5: Algèbre Générale

Groupe de Kholle Paris-Saclay

October 28, 2020

Exercice 1 *H, K sous groupes de $(G,\cdot)$.*
Montrer que HK sous groupe $\iff HK = KH$.

Solution. Si HK est sous groupe de G, alors $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$
Si $HK = KH$ alors $HK \subset G$, non vide car $e_G \in HK$. $HK \cdot (HK)^{-1} = HKKH = HKH = HHK = HK$ donc $HK \cdot (HK)^{-1} \subset HK$ donc HK sous groupe de G #

Exercice 2 *Montrer que $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$*

Solution. Par l'absurde si $\mathbb{Z} + 2\pi\mathbb{Z} = m\mathbb{Z}$ pour un certain $m \in \mathbb{R}^+$
$\exists n \in \mathbb{Z}$ tq $1 = 1 + 2\pi \cdot 0 = mn$
$\exists p \in \mathbb{Z}$ tq $2\pi = 0 + 2\pi = pm$ donc $2\pi = \frac{p}{n} \in \mathbb{Q}$ absurde.
Donc $\mathbb{Z} + 2\pi\mathbb{Z}$ dense. #

Exercice 3 (Lagrange) *Montrer que pour $(G,\cdot)$ fini, H sg de G, $\sharp H \mid \sharp G$*

Solution. On introduit $\mathcal{R}$ la relation sur G donné par $x\mathcal{R}y \iff x^{-1}y \in H$
Réflexivité : $x^{-1}x = e_G \in H$ dc $x\mathcal{R}x$
Symétrie : $x\mathcal{R}y \Rightarrow x^{-1}y \in H \Rightarrow y^{-1}x \in H \Rightarrow y\mathcal{R}x$
Transitivité : $\forall x, y, z \in G, x\mathcal{R}y, y\mathcal{R}z \Rightarrow x^{-1}y \in H, y^{-1}z \in H \Rightarrow x^{-1}yy^{-1}z \in H \Rightarrow x^{-1}z \in H \Rightarrow x\mathcal{R}z$
Donc $\mathcal{R}$ relation d'équivalence, on note $C(x)$ la classe de x.
$y \in C(x) \iff x\mathcal{R}y \iff x^{-1}y \in H \iff y \in xH$ donc $C(x) = xH$
Or $f : h \in H \mapsto xh \in xH$ bijective.
Donc $|H| = |xH|$. Les classes forment une partition de G donc $\exists x_1, \cdots, x_r$ tq
$x_1H, \cdots, x_rH$ partition de G, $G = \bigcup_{i=1}^{r} x_iH$
donc $|G| = \sum_{i=1}^{r} |x_iH| = r|H|$ ie $|H| \mid |G|$ #

Exercice 4 *Pour $(G,\cdot)$ fini, $f : G \to G'$ morphisme.* $|G| = |\ker f| \cdot |\mathrm{Im} f|$

Solution.
•$f(G)$ fini, on note $f(G) = \{y_1, \cdots, y_p\}$
•$f^{-1}(\{y_1\}), \cdots, f^{-1}(\{y_r\})$ forment une partition de G
On note pour chaque i, x_i un élément de $f^{-1}(\{y_i\})$ et on pose :

$$\begin{array}{rccccc} \varphi_i & : & f^{-1}(\{y_i\}) & \to & f^{-1}(\{e_G\}) = \ker f \\ & & x & \mapsto & xx_i^{-1} \end{array}$$

bijective de réciproque $y \mapsto yx_i$
donc $|f^{-1}(\{y_i\})| = |\ker f|$
•$G = \bigcup_{i=1}^{p} f^{-1}(\{y_i\})$ donc $|G| = \sum_{i=1}^{p} |f^{-1}(\{y_i\})| = p|\ker f|$
Bilan, $|G| = |\ker f| \cdot |\mathrm{Im} f|$

Exercice 5 (Théorème de Cauchy) *$(G,\cdot)$ groupe fini, p premier tq $p||G|$. Mq il existe $x \in G$ d'ordre p.*

Solution.
• On note $E = \{(x_1, \cdots, x_p) \in G^p | x_1 \cdots x_p = e_G\}$, $\sigma = (2, 3 \cdots p, 1)$ la permutation circulaire.
On a $x_1 \cdots x_p = e_g \iff x_2 \cdots x_p x_1 = e_G \iff x_{\sigma^k(1)} \cdots x_{\sigma^k(p)} = e_G \ \forall k \in \mathbb{Z}$
• $< \sigma >= \{\mathrm{id}, \sigma, \cdots, \sigma^{p-1}\}$ On note

$$\begin{array}{rccccc} \varphi & : & < \sigma > \times E & \to & E \\ & & (s, x) & \mapsto & s \cdot x & = (x_{s(1)}, \cdots, x_{s(p)}) \end{array}$$

•$|E| = |G|^{p-1}$ (inshallah crois moi)
• Pour $x \in E$, $O(x) = \{s \cdot x | s \in < \sigma >\}$ et on s'intéresse à $|O(x)|$.
1er cas $s \cdot x = x$ alors $x_1 = \cdots = x_p$ donc $|O(x)| = 1$ et $x_1^p = e_G$
2eme cas $s \cdot x \neq x$
Il est clair que les éléments de $O(x)$ sont 2 à 2 distincts, donc $|O(x)| = p$
• On définit sur E la relation $\mathcal{R}$ par $x\mathcal{R}y \iff y \in O(x)$
C'est une relation d'équivalence, donc les orbites forment une partition de E.
E = Union des orbites = Union des orbites de card 1 Union celles de card p
Donc $|G|^{p-1} = |E|$ = nb orbite de card $1 \cdot 1$ + nb orbite de card $\mathrm{p} \cdot p$
Or $p||G|$ donc $p||G|^{p-1}$ donc $p|$nb d'orbite de card 1 et ce nb > 1 car $|O(eg)| = 1$
Donc il y en a au moins p et donc $\exists g \neq e_G$ tq $|O(g, \cdots, g)| = 1$ donc $g^p = e_G$
donc $\mathrm{ord}(g) = p$ #

Exercice 6 *Montrer que les sous groupe d'un groupe cyclique sont cycliques*

Solution. Soit $G =< a >, |G| = n$. Soit H sg de G.
On note $r = \min\{k \in \mathbb{N}^* | a^k \in H\}$ existe car l'ensemble est non vide $\subset \mathbb{N}$.
Donc $a^r \in H$ et donc $< a^r > \subset H$.
Soit $x \in H$, $\exists m \in \mathbb{N}$ tq $x = a^m$. On écrit $m = \alpha r + \beta$. $a^m = a^{\alpha r} a^\beta \Rightarrow a^\beta \in H$
Or $\beta \in \mathbb{N}$ et $\beta < r$ donc $\beta = 0$ et $a^m = x \in < a^r >$ donc H cyclique #

Exercice 7 $G =< a >, |G| = n$, *mq* a^r *génère* G *ssi* $(r, n) = 1$. *En déduire que* G *a* $\varphi(n)$ *générateurs.*

Solution. a^r générateur $\iff \text{ord}(a^r) = n \iff \frac{\text{ord}(a)}{(n,r)} = n \iff (n, r) = 1$
De fait, les générateurs de G sont les a^r tel que $(r, n) = 1, 0 < r < n$ donc $\varphi(n)$ générateurs #

Exercice 8 $G =< a >, |G| = n$, $d|n$. *Montrer qu'il y a* $\varphi(d)$ *élément d'ordre* d. *Montrer qu'il existe un unique sous groupe d'ordre* d.

Solution. Conclusion possible en considérant $H =< a^{\frac{n}{d}} >$
Sinon a^p d'ordre $d \iff \frac{n}{(p,n)} = d \iff (n, p) = \frac{n}{d} \iff \exists k / p = \frac{n}{d} k$ et comme $\frac{n}{d} d = n$, $(k, d) = 1$
Donc $\varphi(d)$ éléments d'ordre d.
Si H sg d'ordre d cyclique donc $\varphi(d)$ génétateurs et ils sont d'ordre d dans H donc dans G. G n'a que $\varphi(d)$ éléments d'ordre d donc ils sont tous dans H #

Exercice 9 (Commutativité de $\mathcal{S}_n$) *Etude de* $Z(\mathcal{S}_n)$

Solution. Pour $n = 1, 2$, $\mathcal{S}_n$ commutatif donc $Z(\mathcal{S}_n) = \mathcal{S}_n$.
Soit $n \geq 3$, pour tout i, j tq $i \leq j$ et pour $\sigma \in Z(\mathcal{S}_n)$ on a:
$\sigma \circ \tau_{i,j} \circ \sigma^{-1} = \tau_{i,j}$ donc $\{\sigma(i), \sigma(j)\} = \{i, j\}$
Pour $\{i, j\} \in \mathcal{P}_2([|1, n|]), \exists k \in [|1, n|] \backslash \{i, j\}$ et $\{i, k\} = \{\sigma(i), \sigma(k)\}; \{j, k\} = \{\sigma(j), \sigma(k)\}$
donc $\{k\} = \{i, k\} \bigcap \{j, k\} = \{\sigma(i), \sigma(k)\} \bigcap \{\sigma(j), \sigma(k)\} = \{\sigma(k)\}$
Par suite, $\sigma(i) = i$, $\sigma(j) = j$, vrai $\forall \{i, j\} \in \mathcal{P}_2([|1, n|])$ donc $\sigma = \text{id}$
Conclusion, $Z(\mathcal{S}_n) = \{\text{id}\}$ pour $n =$ ou $n \geq 3$, et $Z(\mathcal{S}_2) = \mathcal{S}_2$#

Exercice 10 (Théorème de Cayley) *Montrer que tout groupe fini est isomorphe à un sous groupe de $\mathcal{S}_n$ pour un certain $n \in \mathbb{N}$*

Solution. Soit $(G, \cdot)$ fini, $G = \{g_1, \cdots, g_n\}$
On note $\mathcal{T}_g : h \in G \mapsto gh$. C'est une bijection donc $\exists! \sigma \in \mathcal{S}_n$ tq $\mathcal{T}_g(g_i) = g_{\sigma(i)}$.
On note σ_g cette permutation.
$\bullet \forall g, g' \in G,\ \mathcal{T}_{gg'} = \mathcal{T}_g \circ \mathcal{T}_{g'}$
Montrons maintenant que $\varphi : g \in G \mapsto \mathcal{T}_g \in \sigma(G)$ est un morphisme de groupe.
$\forall g, g' \in G, \mathcal{T}_{gg'}(g_i) = g_{\sigma_{gg'}(i)} = \mathcal{T}_g \circ \mathcal{T}_{g'}(g_i) = \mathcal{T}(g_{\sigma_{g'}(i)}) = g_{\sigma_g \circ \sigma_{g'}(i)}$
donc $\sigma_{gg'} = \sigma_g \circ \sigma_{g'}$
• L'application $\psi : g \in G \mapsto \sigma_g \in \mathcal{S}_n$ est donc un morphisme de groupe, injectif car $g \in \ker \psi \iff \sigma_g = \mathrm{id} \iff \mathcal{T}_g = \mathrm{id} \Rightarrow \mathcal{T}_g(e_G) = e_G \Rightarrow g = e_G$
Donc ψ isomorphisme de G sur $\psi(G)$ sous groupe de $\mathcal{S}_n$#

Exercice 11 (Formule du multinôme) *Pour $a_1, \cdots, a_p \in A$ commutant 2 à 2, $n \in \mathbb{N}$, montrer que :*
$$(a_1 + \cdots + a_p)^n = \sum_{\substack{(n_1, \cdots, n_p) \in [|1,n|]^p \\ n_1 + \cdots + n_p = n}} \binom{n}{n_1, \cdots, n_p} a_1^{n_1} \cdots a_p^{n_p}$$
avec $\binom{n}{n_1, \cdots, n_p} = \frac{n!}{n_1! \cdots n_p!}$

Solution. $n \geq 1$
$\bullet (a_1 + \cdots + a_p)^n = (a_1 + \cdots + a_p) \cdots (a_1 + \cdots + a_p)$
Un terme générique s'écrit $a_1^{n_1} \cdots a_p^{n_p}$ avec $n_1 + \cdots + n_p = n$
Pour $(n_1, \cdots, n_p) \in [|0, n|]^p$ tq $n_1 + \cdots + n_p = n$, comptons le nombre de fois où ce facteur apparaît :
$\bullet \binom{n}{n_1}$ choix pour le premier (a_1)
$\bullet \binom{n-n_1}{n_2}$ pour a_2
$\vdots$
$\bullet \binom{n-n_1-\cdots-n_{p-1}}{n_p}$ pour a_p
Et donc au total $\binom{n}{n_1} \cdot \binom{n-n_1}{n_2} \cdots \binom{n-n_1-\cdots-n_{p-1}}{n_p} = \frac{n!}{n_1! \cdots n_p!}$ ie conclusion #

Exercice 12 (Identité de Vandermonde) *Avec une identification polynomiale, établir l'identité de Vandermonde* $\displaystyle\sum_{i=0}^{p} \binom{p}{i}^2 = \binom{2p}{p}$

Solution. Soient $p, q \in \mathbb{N}$
$(1+x)^p (1+x)^q = (1+x)^{p+q}$ donc $\displaystyle\left(\sum_{i=0}^{p} \binom{p}{i} x^i\right) \cdot \left(\sum_{j=0}^{q} \binom{q}{j} x^j\right) = \sum_{i=0}^{p+q} \binom{p+q}{i} x^i$

Le coefficient de x^n est $\sum_{i+j=n} \binom{p}{i}\binom{q}{j} = \binom{p+q}{n}$
Avec $p = q = n$ on retrouve l'identité de Vandermonde. #

Exercice 13 (Méthode Fonctionnelle) *Calcul de* $S = \sum_{k=0}^{n}(k+2)(k+1)\binom{n}{k}$

Solution. On pose $g(x) = (1+x)^n$ et $\varphi = x^2 g(x)$.
Donc $\varphi''(x) = \sum_{k=0}^{n}\binom{n}{k}(k+2)(k+1)x^k$ or $\varphi''(x) = 2(1+x)^n + 4nx(1+x)^{n-1} + n(n-1)(1+x)^{n-2}$
donc $S = \varphi''(1) = 2^{n+1} + 4n2^{n-1} + n(n_1)2^{n-2}$#

Exercice 14 (Utilisation de racine de l'unité) *Calcul de* $S = \sum_{k\leq \frac{n}{p}} \binom{n}{pk}$

Solution. Soit $\omega = e^{\frac{2i\pi}{p}}$, $1 + \omega^r + \cdots + \omega^{r(p-1)} = p$ si $p = \mathrm{ord}(\omega)|r$, 0 sinon.
On note $g(x) = (1+x)^n$, alors $g(1) + g(\omega) + \cdots + g(\omega^{p-1}) = \sum_{k=0}^{n}\binom{n}{k}(1^k + \omega^k +$

$\cdots + \omega^{k(p-1)} = p\sum_{\substack{k=0 \\ p|k}}^{n}\binom{n}{k} = pS$

Ainsi, $S = \dfrac{g(1) + g(\omega) + \cdots + g(\omega^{p-1})}{p}$.
$(1+\omega^k)^n = e^{\frac{ikn\pi}{p}}2^n\cos(\frac{k\pi}{p})^n$
D'où $S = \Re(S) = \sum_{k=0}^{n-1}\dfrac{2^n}{p}\cos(\dfrac{ikn\pi}{p})\cdot\cos(\dfrac{k\pi}{p})^n$#

Exercice 15 *Que dire d'un anneau* $(A,+,\cdot)$ *tq* $\forall x,y \in A, xy \in \{yx, -yx\}$

Solution. Soient $x, y \in A$
1er cas, $xy = yx$ donc commutatif.
2eme cas, $xy = -yx$. $(1+x)y \in \{y(1+x), -y(1+x)\}$
•$(1+x)y = y(1+x) \Rightarrow xy = yx$
•$(1+x)y = -y(1+x) \Rightarrow y + xy = -y - yx \Rightarrow y = -y \Rightarrow xy = -yx = yx$ donc commutatif. Donc A est commutatif #.

Exercice 16 *Soit K un corps, montrer que $P = \{x \in K | \exists n \in \mathbb{N}^*, \exists x_1, \cdots, x_n \in K \text{ tq } x = x_1^2 + \cdots + xn^2\}$ en est un*

Solution. •P stable par addition.
•P stable par produit (assez facile)
• Si $x \in P\backslash\{0\}$ alors x s'écrit $x = x_1^2 + \cdots + x_n^2$, donc $x = x^2x^{-1} = x_1^2 + \cdots + x_n^2$ donc $x^{-1} = (x^{-1})^2(x_1^2 + \cdots + x_n^2) = (x^{-1}x_1)^2 + \cdots + (x^{-1}x_n)^2 \in P$
Donc P est un corps #

Exercice 17 (Radical d'un idéal) *Soit I un idéal de A commutatif. On appelle radical de I l'ensemble $\sqrt{I} = \{x \in A | \exists n \in \mathbb{N}^*, x^n \in I\}$*
a) Montrer que $\sqrt{I}$ est un idéal.
b) Que vaut $\sqrt{\sqrt{I}}$?

Solution. •$\sqrt{I} \in A$
•$I \neq \emptyset$ donc $\sqrt{I} \neq \emptyset$
• Soient $x, y \in \sqrt{I}, \exists m, n \in \mathbb{N}^*$ tq $x^n \in I, y^m \in I$
$(x-y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k(-1)^{n+m-k}y^{n+m-k} \in I$ car $x^k \in I$ si $k \geq n$ et $y^{n+m-k} \in I$ si $n+m-k \geq m \iff n \geq k$
Donc $(x-y)^{m+n} \in I$ donc $x - y \in \sqrt{I}$, ainsi $\sqrt{I}$ sg de A
• Soit $a \in A$, $x \in \sqrt{I}, \exists n \in \mathbb{N}^*$ tq $x^n \in I$
$(ax)^n = (xa)^n = a^nx^n \in aI = I$ donc $xa \in \sqrt{I}$ donc $\sqrt{I}$ idéal de A.
•$\sqrt{I} \subset \sqrt{\sqrt{I}}$
•$x \in \sqrt{\sqrt{I}} \Rightarrow \exists n \in \mathbb{N}^*$ tq $x^n \in \sqrt{I} \Rightarrow \exists n, m \in \mathbb{N}^*$ tq $(x^n)^m \in I \Rightarrow \exists n, m \in \mathbb{N}^*$ tq $x^{nm} \in I$ donc $x \in \sqrt{I}$
Donc $\sqrt{\sqrt{I}} = \sqrt{I}$#

Exercice 18 (Groupe des inversibles) *Déterminer $\mathbb{Z}[\sqrt{2}]^\times$*

Solution. On pose $G = \mathbb{Z}[\sqrt{2}]^\times, G^+ = G \bigcap \mathbb{R}^{*+}$. $\ln : x \in G^+ \to \ln(x) \in \mathbb{R}$ morphisme de $(G^+, \cdot)$ dans $(\mathbb{R}, +)$
Donc $\ln(G^+)$ sous groupe de $\mathbb{R}$
• On note $a = \inf(\ln(G^+) \bigcap \mathbb{R}^{*+})$ donc $e^a = \inf(G^+ \bigcap]1; +\infty[)$ Par l'absurde s'il existe $1 \leq e^a \leq 1 + \sqrt{2}$ alors $\exists p, q \in \mathbb{Z}$ tq $1 \leq e^a \leq p + q\sqrt{2} < 1 + \sqrt{2}$ tq $p + q\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times \bigcap]1; +\infty[$
Si $p = 0, q = 1$ vu l'inégalité mais $\sqrt{2} \notin \mathbb{Z}[\sqrt{2}]^\times$
Si $q = 0, p = 1$ absurde.
Donc p, q non nul, ils sont donc nécessairement de signe différent.
Montrons d'abord que $p - q\sqrt{2} = \frac{1}{p+q\sqrt{2}}$:
Pour $z \in \mathbb{Z}[\sqrt{2}]^\times, z = p + q\sqrt{2}$

•p et q sont uniques : $p+q\sqrt{2}=p'+q'\sqrt{2}\Rightarrow(p-p')^2=2(q-q')^2$ et $\sqrt{2}\notin\mathbb{Q}$ donc $q=q', p=p'$.
• On note $\bar{z}=p-q\sqrt{2}$, on vérifie facilement que $z\bar{+}z'=\bar{z}+\bar{z'}$
•$N(z)=z\bar{z}=p^2-2q^2$. Si z inversible alors $\exists z'$ tq $1=N(zz')=N(z)N(z')$ et $N(z),N(z')\in\mathbb{Z}$ donc $N(z)=\pm1$. Réciproquement, si $N(z)=\pm1$, alors z inversible d'inverse $\pm\bar{z}$ ie c
• 1er cas, $p>0, q<0$ alors $1<p-q\sqrt{2}=\frac{1}{p+q\sqrt{2}}<1\leq p+q\sqrt{2}$ absurde
• 2eme cas, $p<0, q>0$ alors $1<-p+q\sqrt{2}=\frac{1}{p+q\sqrt{2}}\leq 1\leq p+q\sqrt{2}$ absurde.
donc $e^a\geq 1+\sqrt{2}$ et $a\geq\ln(1+\sqrt{2})\in\ln(G^+)\bigcap\mathbb{R}^{*+}(\geq a)$ donc $a=\ln(1+\sqrt{2})$
donc $\ln(G^+)\bigcap\mathbb{R}^{*+}=a\mathbb{Z}$ donc $G^+=e^{an}, n\in\mathbb{Z}$ donc $G=\{\pm e^{an}, n\in\mathbb{Z}\}\#$

Exercice 19 *Déterminer le groupe* $\hom(\mathbb{Z}[\sqrt{2}])$

Solution. • Soit $f\in\hom(\mathbb{Z}[\sqrt{2}])$, $f(0)=0, f(1)=1, f(n+1)=f(n)+1$ donc par récurrence immédiate $f(n)=n\forall n\in\mathbb{N}$
De la même manière $f(n)=n\forall n\in\mathbb{Z}$
Pour $z\in\mathbb{Z}[\sqrt{2}], z=p+q\sqrt{2}$ et $f(z)=f(p)+f(q\sqrt{2})=p+qf(\sqrt{2})$
$f(\sqrt{2})f(\sqrt{2})=f(\sqrt{2})^2=2$ donc $f(\sqrt{2})=\pm\sqrt{2}$
Finalement, $\hom(\mathbb{Z}[\sqrt{2}])=\{f^{\pm}\}$ avec $f^{\pm}(p+q\sqrt{2})=p\pm q\sqrt{2}\#$