L'objectif des notes suivantes est de donner une idée de l'évolution du cours de *troisième année de Licence intitulé Groupes et anneaux 2* délivré à l'Université de Montpellier et d'expliquer quelques compléments ; elles seront publiées sur

`https://webusers.imj-prg.fr/~joao-pedro.dos-santos/Enseignement.html`

après chaque cours. Ces notes ne se substituent pas à la présence, où les idées essentielles seront présentées. [1]

Programme approximatif

Théorie de groupes

1) Rappels et exemples de groupes : les groupes symétriques ($\mathscr{S}_n$), les groupes linéaires généraux ($\mathrm{GL}_n(\mathbf{K})$, où $\mathbf{K} = \mathbf{C}$, $\mathbf{R}$ ou $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$), le groupe diédral $\mathscr{D}_{2n}$.
2) Action d'un groupe sur un ensemble et exemples : $\mathrm{GL}_n(\mathbf{K}) \circlearrowleft \mathbf{K}^n$, $\mathscr{D}_{2n} \circlearrowleft \{\text{côtés d'une } n\text{-gone}\}$, $\mathscr{S}_n \circlearrowleft \{1, \ldots, n\}$, etc. Stabilisateur, orbites et ensemble quotient. Équation de classes.
3) Groupes quotients et sous-groupes distingués. Exemples.
4) Produit semi-direct et exemples dans les groupes linéaires.
5) p-groupes. Théorèmes de Sylow et ses applications.

Théorie des anneaux commutatifs

6) À venir

Voici quelques références qui peuvent vous apporter plus d'informations.

Références

[1] F. Moulin, X. Buff, et al. *Matématiques – Tout en un pour la licence 2*. Troisième édition. Dunod, 2020.

[2] D. Perrin, *Cours d'Algèbre Maths AGREG*. Ellipses, 1996.

1. "Car, à mon avis, ce qu'il y a de terrible, Phèdre, c'est la ressemblance qu'entretient l'écriture avec la peinture. De fait, les êtres qu'engendre la peinture se tiennent debout comme s'ils étaient vivants ; mais qu'on les interroge, ils restent figés dans une pose solennelle et gardent le silence. [...] Autre chose : quand, une fois pour toutes, il a été écrit, chaque discours va rouler de droite et de gauche et passe indifféremment auprès de ceux qui s'y connaissent, comme auprès de ceux dont ce n'est point l'affaire ; de plus, il ne sait pas quels sont ceux à qui il doit ou non s'adresser. Que par ailleurs s'élèvent à son sujet des voix discordantes et qu'il soit injustement injurié, il a toujours besoin du secours de son père ; car il n'est capable ni de se défendre ni de se tirer d'affaire tout seul." Socrate. *Phèdre*.

Cours 1

(19 Janvier 2022).

Notations générales : Sauf mention du contraire, G est un groupe ! On travaillera souvent avec un corps $\mathbf{K}$, qui est choisit parmi $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ ou même $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

1 Pré-requis

Définition 1. Les définitions suivantes doivent être connues.

(1) Les sous-groupes. **Notation :** $H < G$ signifie H est sous-groupe de G.

(2) L'ordre d'un élément g. **Notation :** $\mathrm{ord}(g)$.

(3) Les morphismes et isomorphismes de groupes.

(4) $\mathrm{Ker}\, f$ et $\mathrm{Im}\, f$ pour un morphisme f.

Les résultats suivants doivent être connus.

Théorème 2 (Théorème de Lagrange.)**.** *Soit G groupe fini. $H < G$. Alors $|H|$ divise $|G|$.*

Proposition 3 (Sur l'ordre)**.** *Soit $g \in G$.*

1) Si $\mathrm{ord}(g) = m$, alors $\langle g \rangle$ est sous-groupe d'ordre m isomorphe à $\mathbf{Z}/m\mathbf{Z}$.

2) Si $g^n = e$, alors m divise n.

3) Si $\mathrm{ord}(g) = m$, alors $\mathrm{ord}(g^n) = \dfrac{m}{\mathrm{pgcd}(m,n)}$.

Proposition 4. *Soit $f : G \to G'$ un morphisme de groupes. Alors f est injectif si et seulement si $\ker(f) = \{e\}$.*

2 Quelques exemples de groupes

Dans la suite, on donne quelques exemples que le lecteur connaître.

Exemple 5. 1/ Avec la multiplication usuelle des complexes, $\mathbf{C}^*$ devient un groupe. Le sous-groupe $\boldsymbol{\mu}_n = \{z \in \mathbf{C}^* \,:\, z^n = 1\}$ est le groupe des racines n-èmes de l'unité. Il est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ via le morphisme $f : \mathbf{Z}/n\mathbf{Z} \to \boldsymbol{\mu}_n$ défini par $f(k \mod n) = e^{2\pi \mathrm{i} k/n}$.

2/ Soit $\mathrm{GL}_n(\mathbf{K})$ le groupe des matrices $n \times n$ inversibles. Si $\mathbf{K} = \mathbf{F}_p$, alors GL_n est un groupe fini. Pour déterminer son cardinal, on observe qu'une matrice $X \in \mathrm{GL}_n(\mathbf{F}_p)$ n'est rien d'autre qu'une liste de n vecteurs $[X_1, \ldots, X_n]$ tels que $X_1 \neq 0$, $X_2 \notin \mathbf{K}X_1$,

$X_3 \notin \mathrm{Vect}(X_1, X_2)$, etc. Donc, pour X_1 nous avons $\#\mathbf{F}_p^n = p^n - 1$ choix. Pour X_2, nous avons $\#\mathbf{F}_p^n - \#\{\text{droite}\} = p^n - p$ choix. Pour X_3, nous avons $p^n - p^2$ choix. Donc,

$$\#\mathrm{GL}_n(\mathbf{F}_p) = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}).$$

En particulier, $|\mathrm{GL}_2(\mathbf{F}_2)| = 6$. On vera que $\mathrm{GL}_2(\mathbf{F}_2) \simeq \mathscr{S}_3$.

3/ On fixe $n > 1$. Soit $R \in \mathrm{GL}_2(\mathbf{R})$ la rotation d'un angle $2\pi/n$ dans le sens anti-horaire autour de l'origine. Soit S la réflexion $(x, y) \mapsto (-x, y)$. En identifiant $\mathbf{R}^2 = \mathbf{C}$, on voit que

$$S(z) = \overline{z} \quad \text{et} \quad R(z) = e^{\frac{2i\pi}{n}} \cdot z.$$

Il suit que $SR^kS = R^{-k}$. On affirme que

$$\mathscr{D}_{2n} = \{I, \ldots, R^{n-1}\} \cup \{S, RS, \ldots, R^{n-1}S\}$$

est un sous-groupe de $\mathrm{GL}_2(\mathbf{R})$. On observe que :

$$R^iR^j = R^{i+j}, \quad R^iR^jS = R^{i+j}S, \quad R^iSR^j = R^iR^{-j}S$$

et

$$R^iSR^jS = R^{i-j}.$$

Conséquence : $\mathscr{D}_{2n}$ est stable par multiplication. Pour vérifier que $\mathscr{D}_{2n}$ est stable par la prise des inverses, il suffit de noter que ceci est évident pour $\{I, \ldots, R^{n-1}\}$ et que $R^iS \cdot R^iS = I$. Ce groupe s'appelle le groupe diédral de $2n$ éléments.
De plus : $n > 2$, alors $\mathscr{D}_{2n}$ n'est pas commutatif.

3 Actions

Définition 6. Soit X ensemble. Une *action* de G sur X est une fonction :

$$G \times X \longrightarrow X, \qquad (g, x) \longmapsto g * x$$

telle que

$$e * x = x, \quad \text{et} \quad (gh) * x = g * (h * x).$$

La donnée d'une action de G sur X sera notée souvent par $G \circlearrowleft X$. De temps en temps, un ensemble avec une action sera appelé un *G-ensemble*.

Exercice 7 (Simple mais important)**.** $G \circlearrowleft X$. Alors $T : G \to \mathrm{Bij}(X)$, définie par $T_g = g*x$ est un morphisme de groupes. Réciproquement, si $T : G \to \mathrm{Bij}(X)$ est morphisme, alors $g * x := T(g)(x)$ est action. Souvent on dit que $T_g(x) = g * x$ est la *translation* associée à g.

Les exemples sont multiples et naturels.

Exemple 8. 1/ Le groupe $\mathscr{S}_n$ agit de façon évidente sur l'ensemble $\{1, \ldots, n\}$.

2/ On identifie $\mathbf{K}^n$ avec l'ensemble des vecteurs colonne. Le groupe $\mathrm{GL}_n(\mathbf{K})$ agit sur $\mathbf{K}^n$ par multiplication de matrices : $A * v = Av$.

3/ Pour chaque $g \in \mathscr{D}_{2n}$ et chaque $z \in \boldsymbol{\mu}_n$, l'élément gz est encore une racine de l'unité (ceci se vérifie, algébriquement, en faisant appel à $Rz = e^{2\pi \mathrm{i}/n} \cdot z$ et $Sz = \overline{z}$) et on obtient une action de $\mathscr{D}_{2n}$ sur $\boldsymbol{\mu}_n$.

4/ Si $H < G$, alors H agit sur G par $h * g = hg$. C'est l'action par translations à gauche.

4' Si $H < G$, alors H agit sur G par $h * g = gh^{-1}$. Le lecteur devra vérifier que la formule précédente est la bonne et que en écrivant $h * g = gh$, on *n'obtient pas une action !* Cette action est connue comme l'action par translations à droite.

Dans l'exemple précédent, on a vu que un sous-groupe $H < G$ peut agir de deux façons différentes. Finalement, ces actions ne sont pas si différentes que ça. Pour exprimer cela de façon précise, on a besoin de :

Définition 9. $G \circlearrowright X$ et $G \circlearrowright Y$. Une fonction $f : X \to Y$ est dite *G-équivariante* si $f(g * x) = g * f(x)$ pour tout $g \in G$ et $x \in X$.

On peut maintenant exprimer le fait que les actions par translations à droite et à gauche sont "les mêmes".

Exercice 10. Soit $H < G$. Soit G_{s} l'ensemble G muni de l'action par translations à gauche de H, à savoir, $h *_{\mathrm{s}} x = hx$. Soit G_{d} l'ensemble G muni de l'action par translations à droite de H, à savoir, $h *_{\mathrm{d}} x = xh^{-1}$. Montrer que la focntion $(-)^{-1} : G_{\mathrm{s}} \to G_{\mathrm{d}}$ est une bijection H-équivariante.

Souvent l'action doit préserver une autre structure de X.

Définition 11. 1. Soit Γ un groupe et $G \times \Gamma \to \Gamma$ une action. On dit que G agit par *homomorphismes* si $g*(\gamma\gamma') = (g*\gamma)(g*\gamma')$ pour tout $g \in G$ et $\gamma, \gamma' \in \Gamma$. Dit autrement, T_g (voir l'Exercice 7) est toujours un morphisme de groupes.

2. Soit X un espace vectoriel sur corps $\mathbf{K}$ et $G \times X \to X$ une action. On dit que cette action est linéaire si T_g (comme dans l'Exercice 7) est toujours une application linéaire.

Exemple 12. 1/ G agit sur lui même par translations à gauche. Cette action n'est pas une action par morphismes si $|G| > 1$: en effet, si $g*(xy) = g*x \cdot g*y$, alors $gxy = gxgy$ et donc $x = xg$ et $g = e$.

2/ L'action de $\mathrm{GL}_n(\mathbf{K})$ sur $\mathbf{K}^n$ est clairement linéaire.

L'un des exemples les plus importantes d'actions par morphismes de groupes est le suivant :

Exemple 13 (L'action par conjugaison)**.** Soit $H < G$. On définit, l'action de H sur G par conjugaison en écrivant posant ${}^h g = hgh^{-1}$. Il s'agit d'une action par homomorphismes de groupes :

$$\begin{aligned} {}^h(g_1 g_2) &= h g_1 g_2 h^{-1} \\ &= h g_1 h^{-1} h g_2 h^{-1} \\ &= {}^h g_1 \cdot {}^h g_2. \end{aligned}$$

Il s'agit de *l'action par conjugaison.*

L'idée même d'action donne déjà des résultats non-triviaux.

Théorème 14 (Théorème de Cayley)**.** *Soit G d'ordre n. Alors G est isomorphe à un sous-groupe de $\mathscr{S}_n$.*

Démonstration. On considère l'action de G sur lui même par translations à gauche. D'après l'exercice 7, on obtient un morphisme de groupes $T : G \to \mathrm{Bij}(G) \simeq \mathscr{S}_n$. Or, il est clair que $g \in \mathrm{Ker}(T) \Leftrightarrow T_g(x) = x$ pour tout $x \Leftrightarrow g = e$. Donc T est injectif et $T : G \to \mathrm{Im}(T)$ est isomorphisme. □

Malgré son apparence spectaculaire, le théorème de Cayley n'est pas si puissant que ça : Les sous-groupes d'un groupe symétrique ne sont pas simples à déterminer.

Exemple 15. Soit $\zeta = e^{2i\pi/5}$. On dénombre $\boldsymbol{\mu}_5$ en écrivant $\{\zeta^1, \zeta^2, \ldots, \zeta^5\}$. En laissant μ_5 agir à gauche, on arrive à

$$T : \boldsymbol{\mu}_5 \longrightarrow \mathrm{Bij}(\boldsymbol{\mu}_5) = \mathscr{S}_5, \qquad \zeta^k \longmapsto (1\,2\,\cdots\,5)^k.$$

Cours 2

(19 janvier).

On continue à travailler sur les exemples d'actions.

Définition 16 (Vocabulaire fondamental)**.** $G \circlearrowleft X$. Soit $x \in X$.

(1) Un sous-ensemble $Y \subset X$ est stable par G si $g(Y) \subset Y$ pour tout $g \in G$.

(2) *L'orbite* est le sous-ensemble $O(x) = \{gx \,:\, g \in G\}$. il est clair que $O(x)$ est stable.

(3) Le *stabilisateur* de $x \in X$ est $\mathrm{St}_x = \{g \in G \,:\, gx = x\}$. (Parfois on écrira G_x pour le stabilisateur.) Il est clair que St_x est un sous-groupe.

(4) On dit que x est *point fixe* si $gx = x$ pour tout $g \in G$; l'ensemble des points fixes est noté X^G.

(5) On dit que l'action est *transitive* si X consiste en une seule orbite. Dans ce cas, X est appelé aussi un *espace homogène*.

(6) On dit que l'action est *libre* si les stabilisateurs sont tous réduits à $\{e\}$.

Voici quelques illustrations.

Exemple 17. 1/ $\mathrm{GL}_2(\mathbf{C}) \circlearrowleft \mathbf{C}^2$ de façon standard. Alors $O(\vec{e}_1) = \mathbf{C}^2 \smallsetminus \{0\}$ et $O(\vec{0}) = \{\vec{0}\}$. L'action est transitive sur $\mathbf{C}^2 \smallsetminus \{0\}$ et $\vec{0}$ est l'unique point fixe. Puis :

$$\mathrm{St}_{\vec{e}_1} = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}, \qquad d \neq 0 \right\}.$$

Il suit que $\mathbf{C}^2$ n'est pas un espace homogène et que l'action n'est pas libre.

2/ Il est clair que l'action de G par translations à gauche est libre et transitive.

3/ Soit $H < G$. En laissant H agir par translations à gauche, les stabilisateurs sont triviaux et les orbites sont *les classes à gauche* : $O(g) = Hg = \{hg \,:\, h \in H\}$.

4/ Soit $H < G$. En laissant H agir par translations à droite, les stabilisateurs sont triviaux et les orbites sont *les classes à droite* : $O(g) = gH = \{gh \,:\, h \in H\}$.

Il s'avère que les actions transitives et libres sont "uniques".

Exercice 18. Soit X un G-ensemble avec une action libre et transitive. Soit $x \in X$. Alors $\varphi : G \to X$ défini par $\varphi(g) = g * x$ est une bijection G-équivariante.

4 L'ensemble d'orbites

Le groupe G agit sur un ensemble X.

Définition 19. L'ensemble des orbites de G sera désigné par $G\backslash X$. Il s'appelle le *quotient de X par G*. La fonction qui a $x \in X$ associe son orbite $O(x)$ sera appelée la *projection canonique*.

Exemple 20. (1) Soit $G = \mathrm{GL}_2(\mathbf{R})$; on laisse G agir sur $\mathbf{R}^2$ de façon naturelle : $g \bullet \vec{x} = g(x)$. Il est clair que $G\backslash\mathbf{R}^2 = \{0\} \cup (\mathbf{R}^2 - \{0\})$.

(2) Le groupe $G = \mathbf{R}^*$ agit sur $X = \mathbf{R}^2 - \{\vec{0}\}$ par dilatations : $\lambda * \vec{v} = \lambda\vec{v}$. Ils est clair que les orbites sont de la forme $D - \{\vec{0}\}$, où D est une droite vectorielle.

(3) Soit $H < G$. En laissant H agir par translations à gauche, on obtient l'ensemble quotient des classes à gauche : $H\backslash G$.

(4) Soit $H < G$. En laissant H agir par translations à droite, on obtient l'ensemble quotient des classes à droite : G/H.

Proposition 21. *Soit $H < G$. Il existe une bijection entre les quotients $H\backslash G \to G/H$.*

Démonstration. On a vu que l'inversion $i : G \to G$ définit une bijection H-équivariante (exercice 10). Les orbites sont alors en bijection. □

Exemple 22. On a

$$\mathscr{D}_6/\langle S\rangle = \big\{\{I, S\}, \{R, RS\}, \{R^2, R^2S\}\big\}.$$

Par contre,

$$\langle S\rangle\backslash\mathscr{D}_6 = \big\{\{I, S\}, \{R, R^2S\}, \{R^2, RS\}.\big\}.$$

Définition 23. L'indice de H dans G est le cardinal de l'ensemble G/H, qui est aussi le cardinal de $H\backslash G$. Notation : $[G : H]$. (On ne parlera de $[G : H]$ que quand ce dernier est fini.)

Voici la propriété fondamentale des quotients, dont la preuve est tautologique.

Proposition 24. *Soit X un G-ensemble et Y un ensemble quelconque. Alors, pour chaque fonction $f : X \to Y$ qui est constante sur les orbites, il existe une unique fonction*

$$\overline{f} : X/G \longrightarrow Y$$

tells que $\overline{f}(O(x)) = f(x)$. □

Une propriété très importante du quotient G/H est le fait qu'il vient *encore avec une action*. En effet, on pose

$$g * (xH) = gxH$$

et on vérifie sans effort qu'il s'agit d'une action. Dans la théorie, cette action joue un *rôle prominent car elle est le prototype d'une action transitive.*

Lemme 25. *$G \circlearrowright X$. Soit $x \in X$.*

1) La fonction $\varphi_x : gG_x \mapsto gx$ est bien définie et induit une bijection $G/G_x \to O(x)$.

2) On laisse G agir sur G/G_x comme expliqué ci-dessus et sur $O(x)$ de façon naturelle. Alors la bijection φ_x est G–équivariante.

3) Les stabilisateurs dans une même orbite sont conjugués : $\mathrm{St}_{gx} = g\mathrm{St}_x g^{-1}$.

Démonstration. Évidente, mais on l'a fait pour aider à retenir les définitions.

1. Soit $gG_x = g'G_x$. Alors $g' = gs$ où $s \in G_x$. Donc, $g' * x = g * (s * x) = g * x$. Alors la fonction est bien définie. Elle est surjective par définition d'orbite. Elle est injective car $\varphi_x(gG_x) = \varphi_x(g'G_x) \iff g * x = g' * x \iff g^{-1}g' \in G_x \iff gG_x = g'G_x$.

2. $\varphi_x(h \cdot (gG_x)) = \varphi_x(hgG_x) = hg * x = h * (\varphi_x(g))$.

3. Pour le lecteur. □

Corollaire 26. *Soit X un espace homogène, c'est-à-dire, X n'a qu'une seule orbite. Alors il existe $H < G$ et bijection G-équivariante $\varphi : G/H \to X$.*

Démonstration. On choisit $x \in X$ et on applique le Lemme 25. □

Corollaire 27 (Formules de classe)**.** *G et X finis. $G \circlearrowright X$.*

1. Pour chaque $x \in X$, on a

$$|O(x)| = [G : G_x].$$

2. Soit $O(x_1), \ldots, O(x_q)$ les orbites distinctes. Alors

$$|X| = \sum_{i=1}^{q} |O(x_i)| = \sum_{i=1}^{q} \frac{|G|}{|G_{x_i}|}$$

Démonstration. 1. La fonction $gG_x \mapsto gx$ induit une bijection entre G/G_x et $O(x)$. Donc $|G/G_x| = |O(x)|$. Or, $|G/G_x|$ n'est rien d'autre que $[G : G_x]$.

2. L'ensemble X est réunion disjointe des orbites $O(x_i)$. Donc $|X|$ est $\sum |O(x_i)|$. Chaque $O(x_i)$ possède $[G : G_{x_i}] = |G/G_{x_i}|$ éléments. □

Cours 3

(26 janvier).

Voici quelques illustrations du Corollaire 26.

Exemple 28. 1. Soit P l'ensemble des droites vectorielles de $\mathbf{K}^2$. Le groupe $\mathrm{GL}_2(\mathbf{K})$ agit transitivement sur P. Le stabilisateur de la droite $\mathbf{K}\vec{e}_1$ est le sous-groupe des matrices triangulaires supérieures

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \,:\, ad \neq 0 \right\}$$

et obtient une bijection GL_2-équivariante

$$\mathrm{GL}_2/B \longrightarrow P$$

en utilisant le Lemme 25.

2. Le groupe $(\mathbf{R}, +)$ agit sur le cercle $C = \{c \in \mathbf{C} \,:\, |c| = 1\}$ par rotations : $\theta * c = e^{\mathrm{i}\theta}c$. Clairement, cette action est transitive. De plus, $\mathrm{St}_1 = 2\pi\mathbf{Z}$. La la fonction $\mathbf{R} \to C$ définie par $\theta \mapsto e^{\mathrm{i}\theta} \cdot 1$ établit une bijection entre $\mathbf{R}/2\pi\mathbf{Z}$ et C.

Exemple 29. Soit p un premier et G d'ordre p^n. On note Z son centre. On laisse G agir sur G par conjugaison : $g * x = gxg^{-1}$. On note $\mathrm{Cl}(x)$ l'orbite de $x \in G$; c'est la classe de conjugaison de x. Si $|G|/|\mathrm{St}_x| > 1$, alors $|G|/|\mathrm{St}_x| \equiv 0 \mod p$. Si $|G|/|\mathrm{St}_x| = 1$, il suit que $\mathrm{Cl}(x) = \{x\}$ et donc $x \in Z$. La formule de classes implique :

$$|G| \equiv |Z| \mod p.$$

Par conséquent, $|Z| \equiv 0 \mod p$; en particulier $|Z| \neq 1$. Ceci nous permet de montrer que *tout groupe d'ordre p^2 est abélien*. En effet, si $n = 2$, alors $|Z|$ est soit p ou soit p^2. Si $|Z| = p^2$, on n'a rien d'autre à faire. Sinon, il existe $g \in G - Z$. Soit $C_G(a) = \{g \in G \,:\, ag = ga\}$ le centralisateur de a. Clairement $|C_G(a)| > |Z|$ et donc $C_G(a) = G$. Mais ceci signifie que a commute avec tous les éléments de G, ce qui signifie $a \in Z$, une contradiction.

5 Sous-groupes distingués

Soit H un sous-groupe de G. Il est facile de voir dans le cas où G est abélien, alors les classes à droite et les classes à gauche coïncident. Les sous-groupes ayant cette propriété ont une importance capitale dans la théorie.

Proposition 30. *Soit $H < G$. Les affirmations sont équivalentes :*

(1) Pour chaque $g \in G$, les classes gH et Hg coincident.

(2) Pour tout $g \in G$, le sous-groupe conjugué ${}^gH = gHg^{-1}$ coincide avec H.

(3) Pour tout $g \in G$, le sous-groupe conjugué ${}^gH = gHg^{-1}$ est contenu dans H. □

Démonstration. On prouve facilement que (1) ⇒ (2) ⇒ (3) ⇒ (1). □

Définition 31. Un sous-groupe H de G est distingué quand ${}^gH \subset H$ pour tout $g \in G$; on écrira $H \lhd G$ pour signifier que H est un sous-groupe distingué.

Exemple 32. On a vu à l'exemple 22 que $\mathscr{D}_6/\langle S\rangle = \{\{I, S\}, \{R, RS\}, \{R^2, R^2S\}\}$, mais que $\langle S\rangle\backslash\mathscr{D}_6 = \{\{I, S\}, \{R, R^2S\}, \{R^2, RS\}\}$. Bien évidemment, $R\langle S\rangle R^{-1} = \{I, R^2S\}$, et $\langle S\rangle$ n'est pas distingué.

La façon la plus simple de produire des sous-groupes distingués est par les noyaux (et on vera que finalement c'est la seule).

Lemme 33. *Soit $f : G \to G'$ un morphisme de groupes. Alors* $\mathrm{Ker}(f) \lhd G$.

Démonstration. Soient $x \in \mathrm{Ker}(f)$ et $g \in G$. On a $f(gxg^{-1}) = f(g)f(e)f(g)^{-1} = f(g)f(g)^{-1}$, et ce dernier est e. Donc $gxg^{-1} \in \mathrm{Ker}(f)$. □

Exemple 34. (1) Il est clair que si G est abélien, alors tout sous-groupe est distingué.

(2) Le sous-groupe linéaire spécial $\mathrm{SL}_n(\mathbf{C}) = \{A \in \mathrm{GL}_n(\mathbf{C}) : \det A = 1\}$ est distingué en $\mathrm{GL}_n(\mathbf{C})$ (il est le noyau du morphisme det).

(3) Si $H < G$ est d'indice 2, alors $H \lhd G$; en effet, le fait d'être d'indice deux signifie qu'il existe seulement deux orbites pour l'action de H à droite. Comme une des orbites est $eH = H$, il suit que $G/H = \{ H, G - H \}$. De même, les orbites à gauche sont $\{H, G - H\}$, et $H \lhd G$. Par conséquent, pour chaque $n > 1$, le sous-groupe de $\mathscr{D}_{2n}$ engendré par R est toujours distingué.

(4) Soit $n > 1$. On se rappelle que chaque $\sigma \in \mathscr{S}_n$ possède une signature, notée souvent par $\mathrm{sgn}(\sigma)$, et que sgn : $\mathscr{S}_n \to \boldsymbol{\mu}_2$ est morphisme. Son noyau est appelé le groupe alterné $\mathscr{A}_n$: c'est le groupe des permutations qui s'expriment comme produit d'un nombre pair de transpositions.

Cours 4

(2 février 2022).

On arrive maintenant à la propriété la plus importante des sous-groupes distingués, qui est la possibilité de donner à l'ensemble quotient une structure de groupe. On se donne ainsi H un sous-groupe de G. Si xH et yH sont deux classes distinctes, on peut naïvement définir leur produit par

$$xH \cdot yH = xyH. \tag{†}$$

Mais on observe que si $h, k \in H$, alors $xhH = xH$ et $ykH = yH$, d'où une autre façon de construire leur produit serait

$$xH \cdot yH = xhykH,$$

et (†) n'aura pas de sens si $xyH \neq xhykH$.

Lemme 35. *$H \lhd G$, alors pour chaque couple $h, k \in H$ et chaque couple $x, y \in G$, l'égalité*

$$xyH = xhykH$$

est vraie.

Démonstration. On a

$$xhyk = xy \underbrace{y^{-1}hy}_{\in H} k \quad \Rightarrow \quad xhyk \in xyH.$$

Comme deux classes distinctes sont soit disjointes, soit identiques, on voit que $xhykH = xyH$. □

On peut ainsi énoncer le résultat le plus important concernant les sous-groupes distingués.

Théorème 36. *Soit $H \lhd G$.*

1) *Avec la loi de composition donnée par l'équation (†), l'ensemble G/H est un groupe. L'élément neutre est la classe eH et l'inverse de xH est $x^{-1}H$.*
2) *Soit $\pi : G \to G/H$ la fonction qui à $x \in G$ associe son orbite xH. Alors π est nu morphisme de groupes surjectif et son noyau est H.* □

Soit maintenant $f : G \to G'$ un morphisme de groupes et H un sous-groupe de $\mathrm{Ker}(f)$. D'après la Proposition 24, on déduit une fonction

$$\overline{f} : G/H \longrightarrow G'$$

telle que $\overline{f}(gH) = f(g)$ pour toute classe gH. En effet, puisque $f(h) = e$ pour tout $h \in H$, la fonction f est constante sur les classes gH. En munissant G/H de la structure de groupe construire ci-dessus, il est facile de voir que $\overline{f}$ est en effet un morphisme de groupes :

$$\begin{aligned}\overline{f}(xH \cdot yH) &= \overline{f}(xyH) \\ &= f(xy) \\ &= f(x)f(y) \\ &= \overline{f}(xH)\overline{f}(yH).\end{aligned}$$

Si, de plus, H est précisément le noyau de f, on voit que $\operatorname{Ker}\overline{f} = \{eH\}$: en effet, $\overline{f}(xH) = e$ signifie que $f(x) = e$, c'est-à-dire, $x \in H$. Ceci prouve le simple, mais important résultat suivant :

Théorème 37 (Le noyau et l'image)**.** *Le morphisme* $\overline{f} : G/\mathrm{Ker}(f) \to G'$ *établit un isomorphisme entre* $G/\mathrm{Ker}(f)$ *et* $\mathrm{Im}(f)$.

Ce résultat est très utile pour déterminer efficacement les groupes quotients. (Où "déterminer" signifie, grosso-modo, l'exprimer comme quelque chose déjà connue.)

Exemple 38. (1) Le quotient $\mathscr{S}_n/\mathscr{A}_n$ est isomorphe à $\boldsymbol{\mu}_2$: en effet, $\mathscr{A}_n$ n'est rien d'autre que le noyau de la signature $\mathrm{sgn} : \mathscr{S}_n \to \boldsymbol{\mu}_n$, qui est un morphisme surjectif.

(2) Le quotient $\mathrm{GL}_n(\mathbf{C})/\mathrm{SL}_n(\mathbf{C})$ est $\mathbf{C}^*$, car $\mathrm{SL}_n(\mathbf{C})$ est le noyau du déterminant.

(3) Soit $n > 1$. Le sous-groupe $\mathscr{R} = \langle R \rangle$ de $\mathscr{D}_{2n}$ possède n éléments, d'où $\mathscr{R} \lhd \mathscr{D}_{2n}$. Le quotient est un groupe d'ordre 2, donc isomorphe à $\boldsymbol{\mu}_2$. On observe que $\det : \mathscr{D}_{2n} \to \boldsymbol{\mu}_2$ est un morphisme dont le noyau est $\mathscr{R}$ et $g\mathscr{R} \mapsto \det(g)$ induit un isomorphisme $\mathscr{D}_{2n}/\mathscr{R} \simeq \boldsymbol{\mu}_2$.

(4) Soit X un ensemble avec une action de G et soit $H \lhd G$ tel que $h * x = x$ pour tout $h \in H$ et $x \in X$. Ceci signifie que si $T : G \to \mathrm{Bij}(X)$ désigne la translation (voir Exercice 7), alors $H \subset \mathrm{Ker}(T)$. On en déduit ainsi une action du groupe G/H en utilisant le morphisme $\overline{T} : G/H \to \mathbf{Bij}(X)$. Il est clair qu'une classe gH agit sur x par $gH * x = gx$.

(5) Quelques groupes importants sont décrits comme quotients. C'est le cas des groupes projectifs généraux et spéciaux. Soit $D \lhd \mathrm{GL}_n(\mathbf{K})$ le sous-groupe des multiples non-nuls de l'identité. Le quotient $\mathrm{GL}_n(\mathbf{K})/D$ est le groupe $\mathrm{PGL}_n(\mathbf{K})$. De même, $D \cap \mathrm{SL}_n(\mathbf{K}) \lhd \mathrm{SL}_n(\mathbf{K})$ et $\mathrm{SL}_n(\mathbf{K})/D \cap \mathrm{SL}_n(\mathbf{K})$ est appelé $\mathrm{PSL}_n(\mathbf{K})$.

(6) Soit S^1 le groupe $\{z \in \mathbf{C} : |z| = 1\}$. Pour déterminer le quotient $S^1/\boldsymbol{\mu}_n$, on fait appel au morphisme $[n] : S^1 \to S^1$ définit par $[n](z) = z^n$; clairement $\boldsymbol{\mu}_1 = \mathrm{Ker}([n])$ et, comme $\mathrm{Im}([n]) = S^1$, on déduit que $S^1/\boldsymbol{\mu}_n \simeq S^1$.

Cours 5

(9 février 2022).

Petit oubli terminologique : Si $H \lhd G$ alors le morphisme de groupes $\pi : G \to G/H$ est *la projection canonique* ou *morphisme canonique*.

On prendra le temps de méditer à quelques propriétés des sous-groupes d'un groupe quotient.

Théorème 39. *Soit $N \lhd G$ et $\pi : G \to G/N$ la projection canonique. On écrit $\overline{G} = G/N$.*

(1) Pour chaque $H < G$, l'image $\pi(H)$ est un sous-groupe de $\overline{G}$. De plus, si $H \lhd G$, alors $\pi(H) \lhd \overline{G}$. Le groupe $\pi(H)$ est isomorphe à $H/H \cap N$.

(2) Si $\overline{H}$ est un sous-groupe de $\overline{G}$, alors $\pi^{-1}(\overline{H})$ est l'unique sous-groupe H de G contenant N tel que $\pi(H) = \overline{H}$. De plus, si $\overline{H} \lhd G$, alors $H \lhd G$.

(3) La fonction suivante est une bijection

$$\text{Image} : \left\{ \begin{array}{c} \textit{sous-groupes de } G \\ \textit{contenant } N \end{array} \right\} \longrightarrow \left\{ \textit{ sous-groupes de } \overline{G} \right\}.$$

Démonstration. (1) L'affirmation que $\pi(H)$ est un sous-groupe est évidente. Pour montrer que $\pi(H) \lhd \overline{G}$, on considère $\overline{g} \in \overline{G}$ et $\pi(h) \in \pi(H)$. Soit $g \in G$ tel que $\pi(g) = \overline{g}$. Il suit que $\overline{g}\pi(h)\overline{g}^{-1} = \pi(g)\pi(h)\pi(g)^{-1} = \pi(ghg^{-1})$, et donc $\overline{g}\pi(h)\overline{g}^{-1} \in \pi(H)$.

(2) Clairement $\pi^{-1}(\overline{H})$ est sous-groupe G et comme π est surjective, $\pi(\pi^{-1}(H)) = H$. Soit $K < G$ contenant N et tel que $\pi(K) = \overline{H}$. On note que si $k \in K$, alors $\pi(k) \in \overline{H}$ et donc $k \in \pi^{-1}(\overline{H})$ par définition. On obtient $K \subset \pi^{-1}(\overline{H})$. Ensuite, si $h \in \pi^{-1}(\overline{H})$, il existe $k \in K$ tel que $\pi(k) = \pi(h)$. Par conséquent $\pi(kh^{-1}) \in N \Rightarrow kh^{-1} \in K \Rightarrow h \in K$. On conclut que $\pi^{-1}(\overline{H}) \subset K$ et l'unicité est prouvée. La dernière affirmation est laissée à la charge du lecteur. □

Une autre propriété importante des groupes distingués est qu'ils permettent une compréhension plus efficace des l'opération "groupe engendré par deux sous-groupes".

Proposition 40. *Soit $K \lhd G$ et soit $H < G$. (1) Alors l'ensemble $KH = \{kh : k \in K, h \in H\}$ est un sous-groupe. (2) De plus, si H et K sont finis, alors*

$$|KH| = \frac{|H| \times |K|}{|K \cap H|}.$$

Démonstration. On note que le fait que $K \lhd G$ permet la "règle de commutation" suivante pour $k \in K$ et $h \in H$:

$$\boxed{hk = \underbrace{c_h(k)}_{\in K} h,}$$

on l'on a posé $c_h(x) = hxh^{-1}$. De façon imagée : quand $h \in H$ et $k \in K$ "passent l'un par l'autre , l'élément k devient conjugué." Donc, si $kh \in KH$ et $k'h' \in KH$, alors

$$khk'h' = k \quad \cdot \quad \underbrace{c_h(k')}_{\in K} hh'$$

De même,

$$(kh)^{-1} = h^{-1}k^{-1} = c_{h^{-1}}(k^{-1}) \quad \cdot \quad h^{-1}.$$

Pour (2), soit

$$\phi : K \times H \longrightarrow KH, \quad (k, h) \longmapsto kh.$$

Par définition, ϕ est surjective. Ensuite, sur chaque image réciproque $\phi^{-1}(hk)$, on a précisément $K \cap H$ éléments, à savoir :

$$\{(k \cdot x, x^{-1}h) \, : \, x \in K \cap H\}.$$

En effet, si $k'h' = kh$ alors $k^{-1}k' = hh'^{-1}$ et $x := hh'^{-1}$ est tel que (a) il appartient à $K \cap H$, et (b) $h' = x^{-1}h$, ainsi que $k' = kx$. Le principe du berger termine la preuve. □

Exemple 41.

1. Soit $n > 1$ et $G = \mathscr{D}_{2n}$. Soit $K = \langle R \rangle$ et $H = \langle S \rangle$. On voit que $G = KH$. Dans ce cas, $K \cap H = \{e\}$
2. Soit $G = \mathrm{GL}_2(\mathbf{C})$, $K = \mathrm{SL}_2(\mathbf{C})$, et $H = \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} \, : \, \lambda \in \mathbf{C}^* \right\}$. Alors $G = KH$ et $K \cap H \simeq \boldsymbol{\mu}_2$.

Les groupes ayant la forme décrite précédemment interviennent assez souvent. C'est une version non-commutative des produit directs.

Définition 42. Soit G un groupe, $K \lhd G$ et $H < G$. Si $G = KH$ *et* $K \cap H = \{e\}$, on dira que G est produit semi-direct de K et H. Pour signifier que G est produit semi-direct entre K (qui est distingué) et H (qui est un sous-groupe) j'écrirai

$$G = K \rtimes H.$$

Exemple 43. $\mathscr{D}_{2n} = \langle R \rangle \rtimes \langle S \rangle$.

Cours 6

(15 février 2022).

Soient $K \lhd G$, $H < G$ et on suppose que $G = K \rtimes H$. Si $\pi : G \to G/K$ désigne la projection canonique, alors $\pi : H \to G/K$ est in injective d'après le Thm 39. De plus, comme chaque élément de G a la forme hk avec $h \in H$ et $k \in K$, il suit que π est surjective et $\pi : H \to G/K$ est un iso. *Il suit que H est à la fois un quotient et un sous-groupe de G !* Cette propriété remarquable sert en effet à caractériser les semi-directs.

Théorème 44. *Soient $K \lhd G$ et $H < G$. On suppose que $\pi : H \to G/K$ est un isomorphisme. Alors $G = K \rtimes H$.*

Démonstration. D'abord, $K \cap H = e$; en effet, si $h \in K \cap H \Rightarrow \pi(h) = e$ et puisque $\pi : H \to G/K$ est injective $\Rightarrow h = e$. Ensuite, si $g \in G$, soit $h \in H$ tel que $\pi(h) = \pi(g)$. On déduit que $hK = gK$ et $g = hk$, avec $k \in K$. □

Avec ce point de vue, il est souvent facile d'identifier d'autres prods semi-direct.

Exemple 45. Soit B l'ensemble des matrices triangulaires supérieures de $\mathrm{GL}_n(\mathbf{K})$, à savoir les matrices (b_{ij}) telles que $b_{ij} = 0$ si $i > j$. Il est facile de voir que $B < \mathrm{GL}_n(\mathbf{K})$. Soit U le sous-groupe des matrices triangulaires supérieures *strictes*[2], à savoir, le sous-groupe des matrices $(b_{ij}) \in B$ telles que $b_{ii} = 1$ pour tout i. Finalement, soit T le sous-groupe des matrices diagonales. On vérifie aisément que

$$p : B \longrightarrow T, \quad p(b_{ij}) = \mathrm{diag}(b_{11}, \ldots, b_{nn}).$$

est un morphisme et $U = \mathrm{Ker}\, p$. À partir de là, il est facile de voir que

$$B = UT.$$

En effet, Si $b \in B$, alors $u := b(p(b))^{-1}$ est tel que $p(u) = p(b)p(b)^{-1}$, et donc $u \in U$. Puis, $b = b \cdot p(b)$. Clairment $U \cap T = I$.

Le lecteur aura observé que pour avoir un produit semi-direct, on partait de sous-groupes d'un groupe donné. Or, mais pour construire le produit direct $K \times H$ de deux groupes, on n'a eu recours que à deux groupes abstraits. Le produit semi-direct se laisse également construire dans cet esprit.

Soient ainsi K et H deux groupes *et* une action de H *par morphismes* sur K, définie par le morphisme

$$c : H \longrightarrow \mathrm{Aut}(H), \qquad h \longmapsto c_h.$$

(Le choix de la lettre c n'est pas un accident : il faut penser à la conjugaison.)

2. Attention, parfois on appelle une matrice trinagulaire supérieure stricte, une matrice dont la diagonale est nulle. Ici, notre convention est différente.

Proposition 46. *1. En munissant $K \times H$ de la loi*

$$(k,h) \bullet (k',h') = (k \cdot c_h(k'), hh')$$

on obtient un groupe, noté $K \rtimes_c H$. L'identité de $K \rtimes_c H$ est (e,e) et $(k,h)^{-1} = (c_{h^{-1}}(k^{-1}), h^{-1})$.

2. Pour $k \in K$ et $h \in H$, on écrit $\tilde{k} = (k,e)$ et $\tilde{h} = (e,h)$. Alors

$$\tilde{k} \bullet \tilde{h} = (k,h)$$

et

$$\boxed{\tilde{h} \bullet \tilde{k} = \widetilde{c_h(k)} \bullet \tilde{h}.}$$

3. Soit $\tilde{K} = K \times \{e\}$ et $\tilde{H} = \{e\} \times H$. Alors $\tilde{K}$ et $\tilde{H}$ sont des sous-groupes de $K \rtimes_c H$ et les fonctions

$$K \longrightarrow \tilde{K}, \quad k \longmapsto \tilde{k}$$

$$H \longrightarrow \tilde{H}, \quad h \longmapsto \tilde{h}$$

sont des isomomorphismes.

4. Le sous-groupe $\tilde{K}$ est distingué et $K \rtimes_c H$ est produit semi-direct de $\tilde{K}$ et $\tilde{H}$.

5. La projection $\pi : K \rtimes_c H \to H$ est un morphisme de groupes surjectif et $\tilde{K}$ est son noyau.

6. Soit G' un groupe, $K' \lhd G'$ et $H' < G'$ tels que $G' = K' \rtimes H'$. Soient

$$\phi : K \longrightarrow K' \quad et \quad \psi : H \longrightarrow H'$$

des isomorphismes tels que

$${}^{\psi(h)}[\phi(k)] = \phi[c_h(k)].$$

Alors

$$(\phi, \psi) : K \rtimes_c H \longrightarrow G', \quad (k,h) \longmapsto \phi(h)\psi(h)$$

est iso.

Cours 7

(23/2/2022).

Preuve de la Prp. 46. (1) On vérifie l'associativité seulement. Soient $h_1, h_2, h_3 \in H$, $k_1, k_2, k_3 \in K$. On calcule

$$\begin{aligned}[(k_1, h_1) \bullet (k_2, h_2)] \bullet (k_3, h_3) &= (k_1 c_{h_1}(k_2), h_1 h_2) \bullet (k_3, h_3) \\ &= (k_1 c_{h_1}(k_2) c_{h_1 h_2}(k_3), h_1 h_2 h_3).\end{aligned}$$

De l'autre côté :

$$\begin{aligned}(k_1, h_1) \bullet [(k_2, h_2) \bullet (k_3, h_3)] &= (k_1, h_1) \bullet (k_2 c_{h_2}(k_3), h_2 h_3) \\ &= (k_1 c_{h_1}(k_2 c_{h_2}(k_3)), h_1 h_2 h_3) \\ &= (k_1 c_{h_1}(k_2) c_{h_1 h_2}(k_3), h_1 h_2 h_3)\end{aligned}$$

(2) Par définition :

$$\begin{aligned}(k, e) \bullet (e, h) &= (k c_e(e), eh) \\ &= (k \mathrm{id}(e), h) \\ &= (k, h).\end{aligned}$$

De plus,

$$\begin{aligned}(e, h) \bullet (k, e) &= (e c_h(k), h) \\ &= (c_h(k), h) \\ &= \widetilde{c_h(k)} \bullet \tilde{h}.\end{aligned}$$

(3)–(6) Il s'agit encore de vérifications directes et on s'arrêtera là. □

Exemple 47. 1. Soit $\mathscr{D}_{2n}$ le groupe dihédral. Soit $K = \langle R \rangle$ le sous-groupe engendré par la rotation et $H = \langle S \rangle$ le sous-groupe engendré par la réflexion S et $\mathscr{D}_{2n} = K \rtimes H$. Soit $c : \mathbf{Z}/2 \to \mathrm{Aut}(\mathbf{Z}/n)$ le morphisme définit par $c(\overline{1}) : k \mapsto -k$. Alors En effet,

$$\begin{aligned}SRS^{-1} &= SRS \\ &= R^{-1}.\end{aligned}$$

De plus, on peut même construire un diédral infini : $\mathscr{D}_\infty = \mathbf{Z} \rtimes \mathbf{Z}/2$ où $\mathbf{Z}/2$ agit sur $\mathbf{Z}$ via $k \mapsto -k$.

2. Soit $\zeta_k = e^{2\pi \mathrm{i}/k}$. Il existe un morphisme évident $\varphi : \boldsymbol{\mu}_4 \to \boldsymbol{\mu}_2$ défini par $\varphi(\zeta_4) = \zeta_4^2 = \zeta_2$. On peut ainsi construire un morphisme

$$c : \boldsymbol{\mu}_4 \longrightarrow \mathrm{Aut}(\boldsymbol{\mu}_3), \qquad \zeta_4 \longmapsto (\zeta \mapsto \zeta^{-1}).$$

Soit $G = \boldsymbol{\mu}_3 \rtimes_c \boldsymbol{\mu}_4$. Il s'agit d'un groupe d'ordre $3 \cdot 4 = 12$. On désigne par y l'élément $(\zeta_3, 1)$ de G et par x l'élément $(1, \zeta_4)$. La règle de commutation est alors

$$\boxed{x \bullet y = y^{-1} \bullet x.}$$

On calcule les ordres et on obtient que dans G, il existe un unique élément d'ordre 2. (Exercice !) Il clair aussi que G est non-abélien. Donc G n'est pas isomorphisme ni à $\mathscr{D}_{12}$ (où chaque $R^k S$ est d'ordre 2), ni à $\mathbf{Z}/4 \times \mathbf{Z}/3 \simeq \mathbf{Z}/12$. On a ainsi trouvé un nouveau groupe d'ordre 12.

6 p-groupes et Théorèmes de Sylow

Définition 48. On dit que G est un p-groupe si $|G|$ est une puissance de p. On dit qu'un $P < G$ est un p-sous-groupe de Sylow, ou p-Sylow, si p divise $|G|$, si P est un p-groupe, et si $[G : P]$ est premier à p.

Exemple 49. Soit n un entier > 0. Alors $U_n(\mathbf{F}_p)$, le groupe des matrices triangulaires supérieures strictes (voir Exemple 45) est un p-Sylow de $\mathrm{GL}_n(\mathbf{F}_p)$. En effet, il est facile de construire une bijection

$$\mathbf{F}_p^{n-1} \times \mathbf{F}_p^{n-2} \times \cdots \times \mathbf{F}_p \longrightarrow U_n(\mathbf{F}_p),$$

d'où $|U_n(\mathbf{F}_p)| = p^{n(n-1)/2}$. Ensuite, on sait que

$$|\mathrm{GL}_n(\mathbf{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{n(n-1)/2} \underbrace{\prod_{i=1}^{n} (p^i - 1)}_{\not\equiv 0 \mod p}.$$

On suppose que

$$\boxed{G \text{ a cardinal } p^r m \text{ où } m \not\equiv 0 \mod p.}$$

Théorème 50 (Les théorèmes de Sylow)**.** *Les affirmations suivantes sont vraies.*

i) Le groupe G possède un p-Sylow.

ii) Deux p-Sylows sont toujours conjugués.

iii) Si $H < G$ est un p-groupe, alors H est contenu dans un p-Sylow.

iv) Si n_p note le nombre de p-Sylows de G, alors $n_p | m$

v) Si n_p est comme avant, alors $n_p \equiv 1 \mod p$.

La preuve de l'existence d'un sous-groupe de Sylow sera conséquence de :

Proposition 51. *On suppose que G est sous-groupe d'un groupe fini $\overline{G}$. Si $\overline{P} < \overline{G}$ est un p-Sylow, alors pour un certain $\overline{g} \in \overline{G}$, $\overline{g}\overline{P}\overline{g}^{-1} \cap G$ est p-Sylow.*

Cours 8

(09/03/2022).

On souhaite démontrer les Théorèmes de Sylow. Pour rappel, G est un groupe d'ordre $p^r m$ et $p \nmid m$. Tout dépend de la Prp. 51, qui est notre premier objectif. Elle est une conséquence simple du résultat suivant.

Lemme 52. *Soit X un G-ensemble fini. Si $|X|$ est premier à p, alors il existe une orbite dont le cardinal est premier à p.*

Démonstration. Soient $X_1, \ldots, X_m$ les orbites distinctes. On suppose que $|X_i| \equiv 0 \mod p$ pour tout i. Alors $|X| = \sum_i |X_i| \equiv 0 \mod p$, absurde. □

Démonstration de la Prp 51. G agit sur $\overline{G}/\overline{P}$ par translation : $g * \overline{g}\overline{P} = g\overline{g}\overline{P}$. Clairement, $\mathrm{St}(\overline{g}\overline{P}) = \overline{g}\overline{P}\overline{g}^{-1} \cap G$. Si $G * (\overline{g}\overline{P})$ est une orbite dont le cardinal, qui est $[G : \mathrm{St}(\overline{g}\overline{P})]$, est premier à p, alors $\overline{g}\overline{P}\overline{g}^{-1} \cap G$ est un p-Sylow. □

Démonstration des Théorèmes de Sylow. (i) Tout groupe est (isomorphe à un) sous-groupe d'un $\mathscr{S}_n$ (Thm 14). Mais $\mathscr{S}_n$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbf{F}_p)$. En effet, soit $w : \mathscr{S}_n \to \mathrm{GL}_n(\mathbf{F}_p)$ la fonction

$$\sigma \longmapsto w_\sigma$$

où $w_\sigma \in \mathrm{GL}_n(\mathbf{F}_p)$ est définie par

$$w_\sigma(\vec{e}_j) = \vec{e}_{\sigma(j)}.$$

On voir facilement que w est un morphisme de groupes, qui est injectif et donc $w : \mathscr{S}_n \to w(\mathscr{S}_n)$ est un isomorphisme. On applique ainsi la Prp 51 avec $\overline{G} = \mathrm{GL}_n(\mathbf{F}_p)$ et $\overline{P} = U_n(\mathbf{F}_p)$ pour montrer que G possède un p-Sylow.
(ii) Soient P et Q des p-Sylows. Par le Corollaire 51, il existe ainsi un $g \in G$ tel que $gPg^{-1} \cap Q$ est un p-Sylow de Q, donc $gPg^{-1} = Q$.
(iii) Soit P un p-Sylow de G. Il existe un $g \in G$ tel que ${}^gP \cap H$ est un p-Sylow de H. Or, mais il est clair que H est l'unique p-Sylow de H. Il suit que $H < {}^gP$ et la preuve est terminée car ${}^gP$ est un p-Sylow.
(iv) Soit X l'ensemble des p-Sylows de G sur lequel G agit par conjugaison. D'après (ii), si $P \in X$, alors $X = G * P$ et $\mathrm{St}_P = N_G(P)$, le normalisateur de P. Donc,

$$|X| = [G : N_G(P)] = \frac{[G : P]}{[N_G(P) : P]} = \frac{m}{[N_G(P) : P]},$$

et $|X|$ divise m.
(v) On conserve les notations de l'item précédent. Soit $P \in X$ un p-Sylow ; on laisse P agir sur X par conjugaison. Clairement $O(P) = \{P\}$. Ensuite, soit $P' \neq P$. On sait que

$|O(P')|$ est diviseur de $|P|$, donc soit $|O(P')| \equiv 0 \mod p$, soit $|O(P')| = 1$. Si $|O(P')| = 1$ alors

$$P \subset N_G(P') = \{g \in G : {}^gP' = P'\}.$$

Comme P' est l'unique p-Sylow de $N_G(P')$ (car ils sont tous conjugués à P', et le seul conjugué de P' est P' lui même), ceci montre que $P = P'$, une contradiction. Donc $|O(P')| \equiv 0 \mod p$. La conclusion suit de la formule $|X| = |O(P)| + \sum_{P' \neq P} |O(P')| =$ $1 +$ multiple p. $\square$

Cours 9

(16/3/22).

Les groupes où tous les Sylows sont distingués sont assez simples !

Théorème 53. *1) Si H et K sont des sous-groupes distingués de G tels que $H \cap K = e$, alors $hk = kh$ pour tout $h \in H$ et $k \in K$.*

2) On écrit $|G| = p_1^{m_1} \cdots p_r^{m_r}$, avec $p_1, \ldots, p_r$ des premiers distincts. On suppose que pour chaque i, il existe un unique p_i-Sylow P_i de G. Alors

$$\phi : P_1 \times \cdots \times P_r \longrightarrow G, \quad (x_1, \ldots, x_r) \mapsto x_1 \cdots x_r$$

est un isomorphisme de groupes.

Démonstration. (1)Il suffit de remarquer que pour $h \in H$ et $k \in K$ on a $[h,k] = \underbrace{hkh^{-1}}_{\in K} k^{-1} = h \underbrace{kh^{-1}k}_{\in H}$; d'où $[h,k] = e$. C

(2) Si $i \neq j$ il est clair que $P_i \cap P_j = \{e\}$. Ensuite, comme on sait que tous les p_i-Sylows sont conjugués, l'hypothèse dit que $P_i \lhd G$. Il suit que pour chaque $x_i \in P_i$ et chaque $x_j \in P_j$, l'égalité $x_i x_j = x_j x_i$ est vraie.
ϕ est morphisme. On a

$$\begin{aligned}
\phi((x_1, \ldots, x_r) \bullet (y_1, \ldots, y_r)) &= \phi(x_1 y_1, \ldots, x_r y_r) \\
&= x_1 y_1 x_2 y_2 \cdots x_r y_r. \\
&= x_1 x_2 \cdot y_1 y_2 \cdot x_3 y_3 \cdots x_r y_r \\
&= x_1 x_2 x_3 \cdot y_1 y_2 y_3 \cdot x_4 y_4 \cdots x_r y_r \\
&= \cdots \\
&= x_1 \cdots x_r \cdot y_1 \cdots y_r \\
&= \phi(x_1, \ldots, x_r)\phi(y_1, \ldots, y_r).
\end{aligned}$$

ϕ est injectif. On suppose $x_1 \cdots x_r = e$. On écrit $|G| = p_i^{m_i} q_i$, de sorte que $p_i \nmid q_i$, mais $p_j^{m_j} \mid q_i$ si $i \neq j$. Alors

$$e = (x_1 \cdots x_r)^{q_i} = x_1^{q_1} \cdots x_r^{q_i} = x_i^{q_i}.$$

Donc $\mathrm{ord}(x_i) \mid q_i$ et $\mathrm{ord}(x_i) \mid p_i^{m_1} \Rightarrow \mathrm{ord}(x_i) = 1$. □

On termine avec quelques applications des théorèmes de Sylow.

Il est important ici de faire une brève révision concernant les groupes d'automorphsimes des groupes cycliques. Soit $f : \mu_n \to \mu_n$ un automorphisme et soit $\zeta = e^{2i\pi/n}$. Or, $f(\zeta) = \zeta^k$ est générateur de μ_n et donc $\mathrm{pgcd}(n,k) = 1$. Réciproquement, si $f : \mu_n \to \mu_n$ est définit par $f(\zeta) = \zeta^k$ avec $\mathrm{pgcd}(n,k) = 1$, on voit que $\mathrm{ord}(\zeta^k) = n$ et $\langle \zeta \rangle = \mu_n$. Dit

autrement, $\mathrm{Aut}(\mu_n)$ est un groupe d'ordre $\varphi(n)$, où $\varphi(n)$ est l'indicatrice d'Euler et ses éléments sont définis par les morphismes $f_k : \zeta \mapsto \zeta^k$ avec $\mathrm{pgcd}(k, n) = 1$. (En particulier, $\mathrm{Aut}(\mu_n)$ est commutatif.)

Exemple 54. Soit G un groupe d'ordre 15. On sait que $n_3 = 1, 5$ et $n_5 = 1, 3$. De plus, $n_3 \equiv 1 \mod 3$, donc $n_3 = 1$. De même, $n_5 \equiv 1 \mod 5$, donc $n_5 = 1$. Soit P_3 le 3-Sylow et P_5 le 5 Sylow, Il suit que $G \simeq P_3 \times P_5$ et donc $G \simeq \mu_{15}$.

L'exemple précédent peut être facilement généralisé : si $|G| = pq$, avec $p < q$ des premiers tels que $q \not\equiv 1 \mod p$, alors $G \simeq \boldsymbol{\mu}_{pq}$.

Exemple 55. Soit $|G| = 10$. Il suit que $n_2 = 1, 5$ et $n_5 = 1, 2$. Comme $2 \not\equiv 1 \mod 5$, $n_5 = 1$. Soit ainsi P_5 l'unique 5-Sylow – il est distingué. Soient $\langle\zeta\rangle = P_5$ et $\langle\varepsilon\rangle = P_2$. Soit

$$c : P_2 \longrightarrow \mathrm{Aut}(P_5)$$

la conjugaison. Or, les automorphismes de P_5 sont, id, $\zeta \mapsto \zeta^2$, $\zeta \mapsto \zeta^3$ et $\zeta \mapsto \zeta^4$. Clairement, $\zeta \mapsto \zeta^4 = \zeta^{-1}$ est l'unique d'ordre 2. On voit que $c(\varepsilon) = (-)^{-1}$ ou $c(\varepsilon) = \mathrm{id}$ et donc $G \simeq \mathscr{D}_{10}$ ou $G \simeq \mu_{10}$.

Cours 10

(23/3/22).

On étudiera les anneaux dans cette partie. *Ils seront tous commutatifs.*

Dans ce cours, j'au fait que des rappels du cours *Groupes et anneaux 1* qui a eu lieu au premier semestre. Voici les thèmes qui ont été rappelés :

Définition 56. Un anneau (commutatif) est un triplet $(A, +, \cdot)$ ou‘ A est un ensemble muni de deux fonctions, "addition" $+ : A \times A \to A$ et "multiplication" $\cdot : A \times A \to A$ telles que :

1) $(A, +)$ est un groupe abélien.
2) pour tout triplet $a, b, c \in A$, l'égalité $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ et vraie (l'élément $a \cdot (b \cdot c)$ est noté ainsi $a \cdot b \cdot c$) ;
3) Pour tout couple $a, b \in A$, l'égalité $a \cdot b = b \cdot a$ est vraie.
4) Il existe un élément 1_A tel que $1_A \cdot a = a \cdot 1_A = a$ pour tout $a \in A$;
5) La loi distributive est vraie : $a \cdot (b + c) = a \cdot b + a \cdot c$.

Dans la suite, A désigne toujours un anneau !

Remarques 57. L'élément neutre de $(A, +)$ est désigné par 0. On abuse notation souvent et on écrit 1 au lieu de 1_A. Il est aussi traditionnel d'écrire ab au lieu de $a \cdot b$.

Les exemples suivants sont admis :

1. $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$.
2. Les anneaux de polynômes $A[X]$, $A[X_1, \ldots, X_n]$. *On a fait en cours une brève revision sur la multiplication dans $A[X]$ et $A[X, Y]$.*
3. Les anneaux de l'Analyse : $C^\infty(\mathbf{R}, \mathbf{C})$, etc.

Définition 58. Soit A un anneau. Il sera dit intègre quand $a \cdot b = 0$ implique que soit $a = 0$, soit $b = 0$. Il sera dit un corps quand pour chaque $a \neq 0$ de A il existe un $b \in A$ tel que $a \cdot b = 1$.

Exemple 59. L'anneau $\mathbf{Z}$ est intègre, tout comme $\mathbf{Z}[X_1, \ldots, X_n]$. Les anneaux $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ sont des corps. L'anneau $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est aussi un corps.

Proposition 60. *Soit A un corps. Alors A est intègre.* □

Ensuite, on revise la notion de morphisme entre les anneaux.

Définition 61. Soit B un autre anneua. Un morphisme de A dans B est une fonction $f : A \to B$ telle que

1) f est un morphisme entre les groupes $(A,+)$ et $(B,+)$.

2) f préserve la multiplication : $f(aa') = f(a)f(a')$.

3) f préserve l'unité : $f(1) = 1$.

Exemple 62. Les exemples suivants ont été vus lors du cours au premier semestre. Les morphismes caractéristiques : $\chi : \mathbf{Z} \to A$, les inclusions $\mathbf{Z} \to \mathbf{Q}$, etc. Les morphismes d'évaluation $\varepsilon_a : \mathbf{Z}[X] \to A$, où $a \in A$.

Définition 63. Une A-algèbre est un couple (B, f), où $f : A \to B$ est un morphisme.

Il suit que tout anneau est une $\mathbf{Z}$-algèbre de façon canonique : il suffit de prendre comme morphisme la caractéristique χ. Par contre, $\mathbf{Z}/2\mathbf{Z}$ n'est pas une $\mathbf{Q}$-algèbre : en effet, si $f : \mathbf{Q} \to \mathbf{Z}/2$ est un morphisme, alors $f(1) = f(2 \cdot (1/2)) = f(2) \cdot f(1/2)$; mais $f(2) = f(1) + f(1) = 0$ et on déduit que $f(1) = 0$, ce qui est exclu. Dans plusieurs cas, on dira qu'un certain anneau est une A-algèbre et on laissera le morphisme $A \to B$ sans notation.

L'idée clé que le concept de A-algèbre dégage est la possibilité de "multiplier des éléments de l'algèbre par des éléments de A". Ceci se fait de la façon suivante : si (B, f) est une A-algèbre, alors pour chaque $a \in A$ et $b \in B$ on abuse la notation et on écrit $a \cdot b = f(a)b$.

Définition 64. Soient (B, f) et (C, g) des A-algèbres. Un morphisme d'anneaux $h : B \to C$ est un morphisme de A-algèbres si $hf = g$.

En employant l'abus de notation qui permet de multiplier des éléments d'une A-algèbre par des éléments de a, on déduit l'expression suivante pour les morphismes de A-algèbres : si $h : B \to C$ est un morphisme de A-algèbres, alors pour tout $a \in A$ et $b \in B$, on déduite que

$$\boxed{h(ab) = ah(b);}$$

dit autrement, h est "A-linéaire".

Théorème 65 (Propriété universelle des anneaux de polynômes)**.** *Soit B une A-algèbre et soit* $\mathrm{Hom}_A(A[X_1, \ldots, X_n], B)$ *l'ensemble des A-morphismes. Alors*

$$\mathrm{ev} : \mathrm{Hom}_A(A[X_1, \ldots, X_n], B) \longrightarrow \underbrace{B \times \cdots \times B}_{n}$$

$$\varphi \longmapsto (\varphi(X_1), \ldots, \varphi(X_n))$$

est une bijection. □

Cours 11

(30/03/22).

On reprendra la preuve de la propriété universelle des anneaux de polynômes.

Démonstration. Injectivité. Soient φ et φ' tels que $\varphi(X_i) = \varphi'(X_i)$. On se donne

$$P = \sum_{i_1,\dots,i_n} a_{i_1\dots i_n} X_1^{i_1} \cdots X_n^{i_n} \in A[X_1, \dots, X_n].$$

Alors

$$\begin{aligned}
\varphi(P) &= \varphi\left(\sum_{i_1,\dots,i_n} a_{i_1\dots i_n} X_1^{i_1} \cdots X_n^{i_n} \right) \\
&= \sum_{i_1,\dots,i_n} \varphi(a_{i_1\dots i_n} X_1^{i_1} \cdots X_n^{i_n}) \\
&= \sum_{i_1,\dots,i_n} a_{i_1\dots i_n} \cdot \varphi(X_1^{i_1} \cdots X_n^{i_n}) \\
&= \sum_{i_1,\dots,i_n} a_{i_1\dots i_n} \cdot \varphi'(X_1^{i_1} \cdots X_n^{i_n}) \\
&= \varphi'(P).
\end{aligned}$$

Surjectivité. Soient $b_1, \dots, b_n \in B$. On définit

$$\varphi\left(\sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n} \right) = \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} b_1^{i_1} \cdots b_n^{i_n}.$$

Il n'est pas difficile de voit que $\varphi : A[X_1, \dots, X_n] \to B$ induit un morphisme entre les groupes additifs en question, que $\varphi(1) = 1$ et que $\varphi(a \cdot P) = a \cdot \varphi(P)$ pour tout $a \in A$ et $P \in A[X_1, \dots, X_n]$. Il nous reste la vérification de la propriété

$$\varphi(PQ) = \varphi(P)\varphi(Q). \tag{$\star$}$$

Il est clair que $\star$ est vraie si P ou Q appartient à A. Pour chaque $R \in A[X] \setminus \{0\}$, soit $s(R)$ le "nombre de monômes non-nuls" dans R ; on définit $s(0) = 0$. On fait une récurrence sur $s(P) + s(Q)$; il est clair que $(\star)$ est vraie si $s(P) + s(Q) \leqslant 2$. On suppose $(\star)$ vraie pour tout couple P', Q' tel que $s(P') + s(Q') < s(P) + s(Q)$. On écrit ainsi $P = M + P'$, avec M un monôme et $s(P') < s(P)$. Par hypothèse de récurrence, $\varphi(P'Q) = \varphi(P')\varphi(Q)$ et $\varphi(MQ) = \varphi(M)\varphi(Q)$. Donc

$$\begin{aligned}
\varphi(PQ) &= \varphi(MQ + P'Q) \\
&= \varphi(MQ) + \varphi(P'Q) \\
&= \varphi(M)\varphi(Q) + \varphi(P')\varphi(Q) \\
&= \varphi(P)\varphi(Q).
\end{aligned}$$

□

Une fois cette propriété fondamentale dégagé, on peut facilement introduire la notion de "sous-anneau engendré" par un certain nombre d'éléments. D'abord un rappel :

Définition 66. Un sous-anneau A_0 de A est un sous-groupe A_0 de $(A, +)$ tel que $1_A \in A_0$ e pour tout $a_0, a_0' \in A_0$, leur produit $a_0 a_0'$ est aussi dans A_0.

Il va sans dire que si A_0 est un sous-anneau de A, alors A devient immédiatement une A_0-algèbre.

Exemple 67. 1) $\mathbf{Z}$ est un sous-anneau de $\mathbf{Q}$.

2) Les fonctions constantes forment un sous-anneau de $F(\mathbf{R}, \mathbf{R})$ [3].

3) $\mathbf{Q}[X]$ est un sous-anneau de $\mathbf{Q}[X, Y]$.

4) $2\mathbf{Z} = \{\text{nombres pairs}\}$ n'est pas un sous-anneau de $\mathbf{Z}$: en effet, $1 \notin 2\mathbf{Z}$.

5) Si $f : A \to B$ est un morphisme, alors $\mathrm{Im}(f)$ est un sous-anneau de B.

Définition 68. On suppose A un sous-anneau de B. Soient $b_1, \ldots, b_n$ des éléments de B et soit $f : A[X_1, \ldots, X_n] \to B$ l'unique morphisme d'anneaux tel que $f(X_i) = b_i$. L'image de f est la A–sous-algèbre de B engendrée par $b_1, \ldots, b_n$.

Ceci permet de construire plusieurs anneaux à savoir $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[\sqrt{3}]$, $\mathbf{Z}[\sqrt{-5}]$, etc. Mais le lecteur ayant pris le temps de manipuler ces exemples remarquera immédiatement une certaine inefficacité derrière la construction offerte par la Déf. 68. En effet, $\mathbf{Z}[\sqrt{2}]$ est le sous-anneau de $\mathbf{R}$ ayant des éléments de la forme $\sum_{j=0}^{N} n_j (\sqrt{2})^j$; or, un tel élément peut s'écrire comme $a + b\sqrt{2}$ en s'appuyant sur le fait que $(\sqrt{2})^j \in \mathbf{Z}$ si j est pair. Ceci sera mieux compris à l'aide des idéaux.

3. Oubli : Dans les notes du dernier cours, j'ai oublié de transcrire les exemples des anneaux de fonctions. On écrira $F(X, \mathbf{R})$ pour désigner l'anneau des fonctions d'un ensemble X dans $\mathbf{R}$ avec multiplication et addition naturelles : $fg : x \mapsto f(x)g(x)$ et $f + g : x \mapsto f(x) + g(x)$. Le lecteur n'aura aucun problème à définir les anneaux $F(X, \mathbf{Q})$, $F(X, \mathbf{C})$, etc.

Cours 12

(13/4/22).

Idéaux et quotients

On commence avec des rappels :

Définition 69. Un idéal de A est un sous groupe I de $(A, +)$ qui est, de plus, stable par la multiplication par des éléments arbitraires de A : si $a \in A$ et $x \in I$, alors $ax \in I$. Étant données $a_1, \ldots, a_n$ des éléments de A, on introduit l'idéal qu'ils engendrent comme étant

$$(a_1, \ldots, a_n) = \{a_1x_1 + \cdots + a_nx_n \, : \, x_1, \ldots, x_n \in A\}.$$

Un idéal est principal quand il est engendré par un seul élément.

L'origine du nom "idéal" vient du fait qu'ils jouent un rôle de "nombre idéal" ou "élément idéal". En effet, chaque élément $a \in A$ produit un idéal principal (a), et, en Théorie de Nombres, le manque de factorisation unique en éléments premiers peut-être supplantée par la factorisation unique en idéaux premiers.

Voici quelques façons simples de produire des idéaux. Les vérifications sont laisséEs au lecteur.

Lemme 70. *1) Soit $f : A \to B$ un morphisme. Alors* $\operatorname{Ker} f$ *est un idéal.*

2) Soient I et J des idéaux de A. Alors $I + J = \{x + y \, : \, x \in I, y \in J\}$ est un idéal contenant I et J à la fois. De plus, tout idéal $\mathscr{I}$ de A contenant I et J contient $I + J$.

3) Soient I et J des idéaux de A. Alors l'ensemble des sommes finies $\sum x_iy_i$ avec $x_i \in I$ et $y_i \in J$ est un idéal contenu dans I et J. □

Ensuite, voici quelques exemples concrets :

Exemple 71. 1) Un idéal qui contient 1 est toujours égal à l'idéal A.

2) Les idéaux des $\mathbf{Z}$ sont tous de la forme $n\mathbf{Z}$ pour un certain n : c'est une conséquence de la division Euclidienne.

3) Si K est un corps, alors les uniques idéaux sont $\{0\}$ et K. En effet, si $I \neq \{0\}$, alors il existe un $u \in I \setminus \{0\}$; soit $v \in K$ tel que $uv = 1$. On déduit que $1 \in I$ et $I = A$. Du Lemme 70, on déduit en particulier que morphisme $f : K \to A$, où $A \neq \{0\}$, est injectif. En effet, $\operatorname{Ker} f = \{0\}$ et dans ce cas f est injectif, ou $\operatorname{Ker} f = K$ et dans. ce cas $f(1_K) = 0_A = 1_A$, ce qui est exclu.

4) Si K est un corps, les idéaux de $K[X]$ sont tous de la forme (f). En effet, soit I un idéal non-nul et soit $f \in I \setminus \{0\}$ tel que $\deg(f) \leqslant \deg(g)$ pour tout $g \in I \setminus 0$. On applique la division Euclidienne : $g = qf + r$ où $0 \leqslant \deg r < \deg f$ ou $r = 0$. Comme $r = g - qf \in I$, la possibilité que r soit non-nul est exclue et $f \mid g$.

On va maintenant voir comment obtenir tous les idéaux comme des noyaux. Pour cela, soit I un idéal de A et soit $\overline{A}$ le groupe quotient A/I. (Attention : I est un sous-groupe d'un groupe abélien, donc il est forcément distingué !) Pour chaque $a \in A$, soit $a + I$ la classe à droite qui lui est associée. On définit

$$(a + I) \cdot (b + I) := ab + I.$$

Cette définition indépend des représentants choisis. En effet, on suppose $a' + I = a + I$ et $b' + I = b + I$. Il suit que $a' = a + x$ et $b' = b + y$ avec $x, y \in I$. Donc

$$a'b' = ab + \underbrace{ay + bx + xy}_{\in I}.$$

Par conséquent, $a'b' + I = ab + I$. Donc la multiplication est bien définie. Il est facile de voir que avec $1_{\overline{A}} = 1_A + I$, le on obtient ainsi un anneau et, et de plus la fonction

$$\pi A \longrightarrow \overline{A}, \qquad a \mapsto a + I$$

est un morphisme, dont le noyau est précisément I. C'est la *projection canonique.*

On a vu deux propriétés désirables des anneaux : les anneaux intègres et les corps. Ceci se reflet pour les idéaux.

Définition 72. Soit I un idéal. On dira que I est premier si $I \neq A$ et A/I est intègre. On dira que I est maximal si $I \neq A$ et A/I est un corps.

Avec cette définition, on voit immédiatement que :

Proposition 73. *Un idéal maximal est premier.*

L'exercice suivant est très instructif :

Exercice 74. Soit $I \neq A$ un idéal.

(a) Montrer que I est premier si et seulement si vaut le "Lemme d'Euclide" : étant donnés $x, y \in A$ tels que $xy \in I$, alors soit $x \in I$, soit $y \in I$.

(b) Montrer que I est maximal si et seulement si les uniques idéaux contenant I sont I et A.

Les anneaux $\mathbf{Z}/n\mathbf{Z}$ sont probablement les exemples les plus importants d'anneaux quotients ; comme leur étude était fait au cours "Groupes et Anneaux 1". Le prochain cas, en niveau de difficulté, est celui de $K[X]$, avec K un corps.

On a déjà vu que les idéaux de $K[X]$ sont toujours de la forme (f) pour un certain $f \in K[X]$. Quelles informations supplémentaires peut-on en déduire à propos du quotient $K[X]/(f)$? Pour cela, on a besoin de quelques autres propriétés générales de la théorie des anneaux.

Définition 75 (Propriétés abstraites de divisibilité)**.** (1) On dit que un élément $x \in A$ *divise* un élément $z \in A$ s'il existe un $y \in A$ tel que $xy = z$. Dans ce cas, on écrira $x \mid z$.

(2) Un élément $u \in A$ est *inversible* s'il divise 1. Il est clair que l'ensemble des éléments inversibles est, avec la multiplication de l'anneau, un groupe. Il sera désigné par $A^\times$.

(3) Soit $x \in A$. Un élément $x' \in A$ est dit *associé* à x si $x' = ux$ avec $u \in A^\times$. On écrira $x \overset{\text{ass}}{\sim} y$ pour dire que x est associé à y et on remarquera que $\overset{\text{ass}}{\sim}$ est une relation d'équivalence.

(4) Un élément $x \in A$ est *irréductible* s'il *n'est pas nul ou inversible* et si *chacun de ses diviseurs lui est associé, ou est inversible.*

Exercice 76. Soit A un anneau intègre et $a \in A$ un élément non-nul et non-inversible. Montrer que si $a = bc$, alors soit $b \in A^\times$, soit $c \in A^\times$.

Un polynôme $f \in K[X]$ est inversible s'il est une constante non-nulle.

La division Euclidienne permet de vérifier facilement les critères d'irréductibilité suivants.

Exercice 77. Soit $f \in K[X]$ de degré deux ou trois. Alors f est irréductible si et seulement si f ne possède aucune racine dans K.

Proposition 78. *Soit f un polynôme unitaire de degré $d > 0$. Alors la K-algèbre $A := K[X]/(f)$ est un espace vectoriel de dimension d et une base est $1+(f), X+(f), \ldots, X^{d-1}+(f)$. De plus, les conditions suivantes sont équivalentes.*

a) L'anneau A est un corps. (C'est-à-dire, (f) est maximal.)

b) L'anneau A est intègre. (C'est-à-dire, (f) est premier.)

c) Le polynôme f est irréductible.

Démonstration. Je laisse la première partie de l'énoncé aux lecteurs.

(a)⇒(b) suit du fait que chaque corps est un anneau intègre.

(b)⇒(c) Si f n'est pas irréductible, alors $f = gh$ avec $\deg g < d$ et $\deg h < d$. Il suit que $[g + (f)] \cdot [h + (f)] = 0$ dans A et A n'est pas intègre.

(c)⇒(a) Il suffit de montrer que (f) est maximal. Si Soit I un idéal contenant (f). Soit g un générateur de I. On déduit que $g \mid f$. On déduit que g est soit inversible, et $I = (g)$, ou g est associé à f, et $(g) = (f)$. □

Pour énoncer le prochain Corollaire, on a besoin de la définition suivante. Un $\alpha \in \mathbf{C}$ est algébrique quand il est racine d'un polynôme $F \in \mathbf{Q}[X] \smallsetminus \{0\}$.

Corollaire 79. *Soit $\alpha \in \mathbf{C}$ un nombre algébrique. Alors l'anneau $\mathbf{Q}[\alpha] \subset \mathbf{C}$ est un corps.*

Démonstration. Soit $\varphi : \mathbf{Q}[X] \to \mathbf{C}$ le morphisme de $\mathbf{Q}$-algèbres définit par $X \mapsto \alpha$. Soit $(f) = \operatorname{Ker} \varphi$. Par définition de nombre algébrique, $f \neq 0$. Clairement, f n'est pas une constante et donc $\deg f > 0$. Or, $\mathbf{Q}[\alpha] = \operatorname{Im} \varphi$ est intègre et donc un corps. □

On peut utiliser la construction des corps abstraits donnée par la Prp 78 pour obtenir des corps finis.

Exemple 80. Soit $f = X^2+X+1 \in \mathbf{F}_2[X]$. Il s'agit d'un polynôme irréductible (exercice). Donc $K = \mathbf{F}_2[X]/(f)$ est un corps avec 4 éléments. De même, $\mathbf{F}_3[X]/(X^2+1)$, est un corps avec 9 éléments.

Exercice 81. Construire un corps K avec 8 éléments et ensuite déterminer un générateur du groupe abélien de $K^\times$.

Cours 13

(20/04/2022).

Définition 82. Un anneau A est factoriel s'il est *intègre* et si les propriétés suivantes sont vérifiées

F1. Pour chaque $f \in A$, il existe des éléments irréductibles $p_1, \dots, p_m$, pas forcément distincts, tels que $f = p_1 \cdots p_m$.

F2. Si $p_1, \dots, p_m$ et $q_1, \dots, q_n$ sont irréductibles, pas forcément distincts, tels que $p_1 \cdots p_m = q_1 \cdots q_n$, alors $m = n$ et il existe $\sigma \in \mathscr{S}_m$ tel que $q_i \overset{\text{ass}}{\sim} p_{\sigma(i)}$.

Exemple 83. L'anneau $\mathbf{Z}$ est l'anneau factoriel par excellence. Ce fait est connu comme "le théorème fondamental de l'arithmétique".

Exemple 84 (**F1** fait défaut)**.** Soit $\mathscr{O}$ l'anneau des fonctions holomorphes sur tout le plan complexe. Soit $f : \mathbf{C} \to \mathbf{C}$ définie par $f(z) := \sin(\pi z)$. En écrivant $t_n(z) = z - n$ pour chaque $n \in \mathbf{Z}$, on voit que $t_n \mid f$ pour tout n. Ceci montre que f ne possède pas de décomposition en facteurs irréductibles.

Exemple 85 (**F2** fait défaut)**.** On peut prendre l'exemple de $\mathbf{Z}[\mathrm{i}\sqrt{5}]$ et décomposer 6 de deux façons différentes : $2 \cdot 3 = (1 - \mathrm{i}\sqrt{5})(1 + \mathrm{i}\sqrt{5})$.

À ce moment, le lecteur devra se rappeler de la preuve du fait que $\mathbf{Z}$ est factoriel. La vérification de **F1** est immédiate et employe la fait que $\mathbf{Z}$ est ordonné. La validité de **F2** est plus subtile et est conséquence des propositions suivantes :

P1 Division Euclidienne $\Rightarrow$ Tout idéal est principal.

P2 Tout idéal est principal $\Rightarrow$ Lemme d'Euclide [4].

P3 Lemme d'Euclide $\Rightarrow$ l'unicité.

Il est ainsi important de pousser les propositions ci-dessus dans un contexte abstrait. Pour simplifier la théorie, on supposera désormais que A est intègre.

La division euclidienne devient un axiome :

Définition 86 (Anneau euclidien)**.** Soit A intègre. Un jauge euclidien est une fonction $\varphi : A \smallsetminus \{0\} \to \mathbf{N}$ ayant la propriété suivante :

DE. Pour chaque couple d'éléments $x \in A$ et $d \in A \smallsetminus \{0\}$, il existe un [5] couple $q, r \in A$ tel que

$$x = dq + r \quad \text{et} \quad \text{si } r \neq 0, \text{ alors } \varphi(r) < \varphi(d).$$

4. Le Lemme d'Euclide est un fait fondamental de l'arithmétique élémentaire : Si p est un nombre premier qui divise un produit ab, alors soit $p \mid a$, soit $p \mid b$.

5. On ne demande pas l'unicité !

Un anneau intègre avec un jauge euclidien est dit un anneau euclidien.

Exemple 87. Les exemples les plus importants d'anneaux euclidiens sont :

(a) L'anneau des entiers avec le jauge $|\bullet|$.

(b) L'anneau des polynômes en une variable $k[X]$ avec le jauge deg. (Ceci est normalement vu au cours d'Arithmétique de L2.)

(c) L'anneau des entiers de Gauss $\mathbf{Z}[\mathrm{i}]$ avec la norme $N(a+\mathrm{i}b) = a^2+b^2$. (Ce fait est moins célèbre que les autres, mais il a été traité aux TDs du cours "Groupes et anneaux" en L3.)

Les anneaux n'ayant que des idéaux principaux gagnent aussi un nom :

Définition 88. A est dit principal si tout idéal est principal, i.e. engendré par un élément.

P1 a été faite au premier semestre :

Théorème 89. *Si A est Euclidien, alors tout idéal est principal.* □

Les éléments pour lesquels l'analogue du Lemme d'Euclide est vrai ont besoin d'un nom :

Définition 90. Un élément $p \in A$ est premier si p n'est pas inversible et s'il jouit de la propriété suivante : si $p \mid ab$ alors p divise soit a, soit b."

Exercice 91. Tout premier est irréductible.

Maintenant **P2** suit :

Théorème 92. *Soit A principal. Alors tout irréductible est premier.*

Démonstration. Soit $x \in A$ irréductible tel qeu $x \mid yz$. On suppose que $x \nmid y$ et on considère un générateru g de $\langle x, y\rangle$. Il suit que $g \mid x$. Dans ce cas, soit $g = ux$ avec $u \in A^\times$, soit $g \in A^\times$. Or, si $x = ug$, il suit que $x \mid y$, ce qui est exclu. Donc $g \in A^\times$ et on peut écirre $1 = ax + by$. Par conséquent, $z = axz + b \cdot yz$ et $x \mid z$. □

Finalement, **P3** :

Théorème 93. *Soit A un anneau intègre où tout irréductible est premier. Soient $p_1, \dots p_m$ et $q_1, \dots, q_n$ des irréductibles pas forcément distincts. Alors l'égalité*

$$p_1 \cdots p_m = q_1 \cdots q_n$$

implique que

(i) Les entiers m et n coïncident.

(ii) Il existe $\sigma \in \mathscr{S}_m$ telle que q_j et $p_{\sigma(j)}$ sont associés.

*En particulier, si A est intègre et **F1** est vraie, alors A est factoriel.*

Démonstration. On fait une récurrence sur $\min(m,n)$. Si $m = 1$, on a $p_1 = q_1 \cdots q_n$. Comme p_1 est premier, il doit diviser un certain q_j ; on suppose ainsi que $p_1 \mid q_1$. Dans ce cas, $p_1 \sim q_1$. Puisque A est intègre $\Rightarrow 1 = q_2 \cdots q_n$ et ceci contredit le fait que q_i soit irréductible. Donc $n = 1$. Le cas général est au lecteur.

La dernière affirmation est facile, puisque on a prouvé que la propriété **F2** est vraie. □

On souhaite prouver :

Théorème 94. *Si A est factoriel, alors $A[X]$ l'est aussi.*

7 La factorisation dans un anneau de polynômes

La première étape vers le Thm. 94 est la construction du corps de fractions.

Définition 95. Soit R un anneau intègre. On introduit sur l'ensemble $R \times (R \smallsetminus \{0\})$ la relation d'équivalence $\sim$ suivante :

$$(a,b) \sim (a',b') \iff ab' = a'b.$$

L'ensemble des classes d'équivalence est appelé $\mathrm{Fr}(R)$ et la classe de (a,b) sera désignée par $\dfrac{a}{b}$.

Exercice 96. Vérifier que avec les règles d'addition et multiplication standards, $\mathrm{Fr}(R)$ devient un corps, et que $A \to \mathrm{Fr}(R)$ définie par $a \mapsto \dfrac{a}{1}$ est un morphisme injectif d'anneaux.

Exemple 97. $\mathrm{Fr}(\mathbf{Z}) = \mathbf{Q}$. Le corps de fractions de $\mathbf{C}[X]$ est l'anneau de fractions rationnelles : les "quotients" $p(X)/q(X)$ avec $q(X) \in \mathbf{C}[X] \smallsetminus \{0\}$.

Exercice 98 (Pour les motivés)**.** Soit $\mathscr{O}$ l'anneau des fonctions holomorphes $f : \mathbf{C} \to \mathbf{C}$; la propriété de continuation analytique permet de montrer que $\mathscr{O}$ est intègre. Soit $\mathscr{M}$ le corps des fonctions méromorphes [6] sur $\mathbf{C}$. Quel est le lien entre $\mathscr{M}$ et $\mathrm{Fr}(\mathscr{O})$? (La réponse est donnée dans la section 2.3 du grand classique d'Analyse Complexe de Ahlfors.)

Soit A intègre et $K = \mathrm{Fr}(A)$. À l'aide de K, on pourra faire appel au fait que $K[X]$ est factoriel pour montrer le Thm. 94. L'idée principale ici est utiliser le *contenu d'un polynôme*. On fera ce chemin en empruntant la route ouverte par la *valuation de Gauss*.

6. Soit $U \subset \mathbf{C}$ ouvert. Une fonction méromorphs sur U est la donnée d'un couple (f,P), où $P \subset U$ est discret, $f : U \smallsetminus P \to \mathbf{C}$ est holomorphe, et f n'a qu'un pôle sur chaque $p \in P$.

Soit $\mathscr{P}$ un ensemble de premiers (=irréductibles) de A ayant la propriété suivante : Pour chaque irréductible π de A, il existe un *unique* élément $p \in \mathscr{P}$ associé à π. Avec cette convention, on voit que chaque élément de $A \smallsetminus \{0\}$ s'écrit uniquement comme

$$u \cdot \prod_{p \in \mathscr{P}} p^{v_p}, \quad u \in A^\times, \quad v_p \in \mathbf{N}.$$

Pour chaque $p \in \mathscr{P}$, on peut ainsi introduire la fonction $v_p : A \smallsetminus \{0\} \to \mathbf{N}$ qui à chaque élément associe l'exposant de p dans sa décomposition. Dit autrement :

$$v_p(f) = \max\{n \in \mathbf{N} \,:\, p^n \mid f\}.$$

Comme A est factoriel, il est immédiat de voir que

$$v_p(ab) = v_p(a) + v_p(b).$$

On prolonge v_p à $K \smallsetminus \{0\} \to \mathbf{Z}$ en écrivant

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Il est utils de décréter $v_p(0) = \infty$, où $\infty \geqslant n$ pour chaque $n \in \mathbf{Z}$.

Exemple 99. (1) Soit $A = \mathbf{Z}$. Alors $v_2(3) = 1$, $v_2(1/36) = -2$.

(2) Soit $A = \mathbf{C}[X]$ et $p = X - 1$. Alors $v_p(X^2 - 1) = 1$ et $v_p(1/(X^3 - 1)) = -1$.

Une autre propriété fondamentale de v_p est :

Lemme 100. *$a, b \in K$. Alors :*

(1) On a

$$v_p(a + b) \geqslant \min(v_p(a), v_p(b)).$$

(2) De plus, si $v_p(a) < v_p(b)$, alors $v_p(a + b) = \min(v_p(a), v_p(b))$.

Démonstration. On traite d'abord le cas $a, b \in A$.

(1) On suppose $v_p(a) \leqslant v_p(b)$. Or, $p^{v_p(a)} \mid a + b$ et donc $v_p(a) \leqslant v_p(a + b)$.

(2) Si $v_p(a) < v_p(b)$, alors $p^{v_p(a)+1} \nmid a + b$ car autrement, $a \equiv a + b \equiv 0 \mod p^{v_p(a)+1}$.

Le cas $a, b \in K$ se traite en écrivant $a = a_0/d$ et $b = b_0/d$. □

Cours 14

(27 avril 2021).

Le lecteur n'aura aucun souci à établir le résultat suivant.

Lemme 101. *Soit $a \in K - \{0\}$. Alors $a \in A$ si et seulment si $v_p(a) \geqslant 0$ pour tour $p \in \mathscr{P}$.*

Définition 102. Soit ∞ un symbole tel que $\infty \geqslant n$ pour chaque $n \in \mathbf{Z}$. Une fonction $v : K \to \mathbf{Z} \cup \{\infty\}$ satisfaisant

V0 $v(x) = \infty$ si et seulement si $x = 0$.

V1 $v(ab) = v(a) + v(b)$.

V2 $v(a + b) \geqslant \min(v(a), v(b))$

est appelée une valuation.

On prolonge v_p à $K[X]$.

Définition 103 (La valuation de Gauss)**.** Pour chaque $f = a_n X^n + \cdots + a0 \in A[X]$, on définit :

$$v_p\left(a_n X^n + \cdots a_0\right) = \min\{v_p(a_i)\}.$$

Exemple 104. $v_2(\frac{3}{4}X^3 + 2X^2 - \frac{1}{8}X + 1) = -3$.

Voici une propriété évidente de v_p.

Lemme 105. *Soit $f \in K[X]$. Alors pour tout $\lambda \in K$, on a $v_p(\lambda f) = v_p(\lambda) + v_p(f)$.*

Démonstration. Il suffit de voir que $\min\{v(\lambda) + v(a_i)\} = v(\lambda) + \min\{v(a_i)\}$. □

Ensuite, sa propriété la plus importante.

Théorème 106 ("Lemme de Gauss")**.** *Pour chaque couple de polynômes $f, g \in K[X]$, l'égalité*

$$v_p(fg) = v_p(f) + v_p(g)$$

est vraie.

Démonstration. J'écris v au lieu de v_p. On suppose que $v(f) = v(g) = 0$ pour commencer. On écrit $f = \sum_{i=0}^{\infty} a_i X^i$ et $g = \sum_{j=0}^{\infty} b_j X^j$, où $a_i = 0$, respectivement $b_j = 0$, sauf pour un nombre fini de valeurs de i, respectivement j. Comme pour i très grand, le coefficient a_i est nul, on voit que $v(a_i) > 0$ pour i très grand. Soit ainsi

$$m = \max\{i \,:\, v(a_i) = 0\}.$$

Dit autrement,

$$f = a_0 + \cdots + \underbrace{a_m}_{v=0} X^m + \underbrace{a_{m+1}}_{v>0} X^{m+1} + \cdots$$

De même, soit $n = \max\{i \in \mathbf{N} : v(b_i) = 0\}$. On écrit $fg = \sum_i c_i X^i$ et on note que

$$\begin{aligned} v(c_r) &= v(a_0 b_r + \cdots a_r b_0) \\ &\geqslant \min\{v(a_0 b_r), \ldots, v(a_r b_0)\} \\ &\geqslant 0. \end{aligned}$$

Ensuite, si $m, n > 0$, alors

$$c_{m+n} = \underbrace{a_0 b_{m+n} + a_1 b_{m+n-1} + \cdots + a_{m-1} b_{n+1}}_{v>0} + \underbrace{a_m b_n}_{v=0} + \underbrace{a_{m+1} b_{n-1} + \cdots + a_{m+n} b_0}_{v>0}.$$

Proposition 101-(2) $\Rightarrow v(c_{m+n}) = 0$. Donc, $\min\{v(c_i)\} = 0$. On remarquera que le "$m = 0$ ou $n = 0$" a été laissé de côté, mais le lecteur peut facilement les prouver avec la méthode précédente.

Finalement, on abandonne l'hypothèse $v(f) = v(g) = 0$. On écrit $f = p^{v(f)} \tilde{f}$ et $g = p^{v(g)} \tilde{g}$ avec $v(\tilde{f}) = v(\tilde{g}) = 0$. Il suit que $v(\tilde{f}\tilde{g}) = 0$. Or, $v(fg) = v(p^{v(f)+v(g)} \cdot \tilde{f}\tilde{g})$, et comme $v(p^r) = r + v(h)$, le cas général en découle. □

Il est utile d'introduire maintenant :

Définition 107. On appellera un $f \in K[X]$ p-primitif si $v_p(f) = 0$. Si f est p-primitif pour tout $p \in \mathscr{P}$, on dira que f est primitf.

Quelques remarques à propos des polynômes primitifs :

Lemme 108. *1. Si $f \in K[X]$ est primitif, alors $f \in A[X]$.*

2. Si $f \in A[X]$ est irréductible (et sont degré est > 0), alors f est primitif.

Corollaire 109 (Permanence de l'irréductibilité)**.** *Soit $f \in A[X]$ un polynôme irréductible de degré strictement positif. Alors il est aussi irréductible en $K[X]$.*

Démonstration. Comme f est irréductible, il doit être primitif (Lemme 108). Soit

$$\mathbf{Fact} = \left\{ (g,h) \in K[X] \times K[X] : \begin{array}{c} 0 < \deg g < \deg f \\ 0 < \deg h < \deg f \\ f = gh \end{array} \right\}$$

Pour $(g,h) \in \mathbf{Fact}$, soit $P(g,h) \subset \mathscr{P}$ l'ensemble fini de premiers tels que $\min\{v_p(g), v_p(h)\} < 0$: c'est-à-dire, au moins un des coefficients de g ou h possède un dénominateur divisible

par p. Si $\mathbf{Fact} \neq \varnothing$, on va construire $(\tilde{g}, \tilde{h}) \in \mathbf{Fact}$ tel que $P(\tilde{g}, \tilde{h}) = \varnothing$. Ceci produit une contradiction, car si $\min(v_p(\tilde{g}), v_p(\tilde{h})) \geqslant 0$ pour tout p, alors $\tilde{g} \in A[X]$ et $\tilde{h} \in A[X]$.

Soit $p \in P(g, h)$. Comme $v_p(f) = 0$, on déduit que $v_p(g) = -v_p(h)$. On écrit $g = p^{v_p(g)} g_1$ et $h = p^{v_p(h)} h_1$ où $v_p(g_1) = v_p(h_1) = 0$. Il suit que $f = g_1 h_1$ et $v_p(g_1) = v_p(h_1) = 0$. On obtient $(g_1, h_1) \in \mathbf{Fact}$ tel que $|P(g_1, h_1)| < |P(h, g)|$. Par récurrence, on obtient $(\tilde{g}, \tilde{h}) \in \mathbf{Fact}$ tel que $P(\tilde{g}, \tilde{h}) = \varnothing$. □

On arrive finalement à notre objectif :

Démonstration Théorème 94. On montre que tout irréductible est premier et on utilise Lemme 93 pour assurer que **F2** de la Définition 82 est vraie. Soit $f \in A[X]$ irréductible. Il est en particulier primitif et le Théorème 109 prouve que f est irréductible aussi dans $K[X]$. On suppose $f \mid gh$ dans $A[X]$. Alors $f \mid gh$ dans $K[X]$. Comme f est premier de $K[X]$, on peut supposer que $f\varphi = g$ pour un certain $\varphi \in K[X]$. Or, mais $v_p(\varphi) = v_p(g)$ pour tout $p \in \mathscr{P}$ et $v_p(g) \geqslant 0$, ce qui implique que $\varphi \in A[X]$.

Pour terminer, on doit montrer **F1**. Ceci est plus simple, mais par manque de temps, j'ai omis la preuve. □