ALGÈBRE ET GÉOMÉTRIE

COURS DE M1, PREMIER SEMESTRE 2018/2019

J. Sauloy [1]

September 3, 2018

[1]Institut mathématique de Toulouse et U.F.R. M.I.G., Université Paul Sabatier, 118, route de Narbonne, 31062 Toulouse CEDEX 4

Utilisation du cours

La partie la plus utile du travail consiste probablement à revoir les notes prises pendant le cours en en mettant au propre la rédaction, en vérifiant toutes les assertions et leurs preuves, et, au besoin, en les complétant. Le polycopié n'est qu'un auxiliaire.

À ce sujet, mentionnons qu'une enquête menée les deux dernières années auprès des étudiants de M1 a permis de quantifier la notion qu'ils avaient du travail *nécessaire* pour profiter de l'enseignement reçu: notons (pour n'influencer personne) a le nombre d'heures par semaine (nécessaires) ainsi estimé. La même enquête a permis de quantifier le travail *effectif* fourni, mettons (pour ne dénoncer personne) b le nombre d'heures par semaine (effectives). On observe alors l'égalité approximative:

$$b \simeq 0,5a.$$

Il n'est pas nécessaire d'aller plus loin pour comprendre les difficultés rencontrées par les étudiants de M1. *Il n'y a pas de voie royale.*

Exercices et TD

Une partie des exercices est donnée dans le texte, au fil de l'eau: ils ne seront pas corrigés. Ceux qui sont rassemblés dans la dernière section de chaque chapitre constituent les TD. Il y a une première série, que tout étudiant devrait intégralement aborder; et une deuxième série, pour les plus motivés. Rappelons que c'est la recherche qui est fructueuse et non la lecture de la solution. *Un exercice dont on a lu la solution avant de l'avoir cherchée est perdu pour toujours.*

Bibliographie

Les principaux ouvrages généraux recommandés sont les suivants:

1. Le livre "Algebra" de Serge Lang, champion toutes catégories.
2. Le "Cours de mathématiques pures et appliquées" de Ramis-Warusfel, que l'on citera RW3: niveau L3-M.

Signalons aussi parmi les références recommandables: "Algebra" de Michael Artin et "Cours d'algèbre" de Roger Godement.

Pour le lecteur qui souhaite aller au delà, on peut suggérer, à un niveau encore élémentaire:

1. Le livre "Basic Algebra" de Nathan Jacobson.
2. Les chapitres 4 et 7 du livre "Algèbre" de Bourbaki.
3. Le "Cours de géométrie algébrique élémentaire" de Jean Giraud (quand il sera publié ...).

Ajoutons, pour la partie sur les groupes, deux livres magnifiques de Serre, "Représentations linéaires des groupes finis" (le premier chapitre) et le célèbre "Cours d'arithmétique" (une partie du chapitre sur le théorème de Dirichlet); pour la partie sur les corps, le très clair et très complet "Corps commutatifs et théorie de Galois" de Tauvel; pour la partie sur les modules, le "Algebra" de Lang et le chapitre 4 de la première partie de RW3 (qui contient des indications bibliographiques

supplémentaires); et, pour la partie sur les courbes, le chapitre 4 de la deuxième partie de RW3, qui contient des indications bibliographiques supplémentaires, parmi lesquelles: le cours de Giraud, les livres de Walker et de Fulton tous deux intitulés “Algebraic Curves”, le livre de Shafarevich “Basic Algebraic Geometry” et le manuel de briançon-Maisonobe “Algèbre commutative, M1”.

Conventions générales

La notation $A := B$ signifiera que le terme A est défini par la formule B. Les expressions nouvelles sont écrites en *italiques* au moment de la définition. Noter qu'une définition peut apparaitre au cours d'un théorème, d'un exemple, d'un exercice, etc.

Exemple 0.0.1 L'espace vectoriel $E^* := \mathrm{Hom}_K(E,K)$ est appelé *dual* de E.

La fin d'une démonstration ou son absence est indiquée par le signe □

Disclaimer

Le syllabus de ce module a été conçu alors que le cours se faisait en 32 heures, avec 36 heures de TD. L'horaire actuel est de 22 heures de cours, avec 32 heures de TD, le syllabus n'ayant, lui, pas changé ! Le cours réellement présenté sera donc violemment élagué.

Part I

Groupes

Chapter 1

Actions de groupes

1.1 Définitions, exemples, vocabulaire

Soient G un groupe noté multiplicativement (en particulier, le neutre sera noté 1) et X un ensemble.

Définition 1.1.1 Une *action (à gauche)* du groupe G sur l'ensemble X est une application

$$\begin{cases} G \times X \to X, \\ (g,x) \mapsto g.x, \end{cases}$$

satisfaisant aux axiomes:

1. $\forall x \in X\ ,\ 1.x = x$;
2. $\forall g,h \in G\ ,\ \forall x \in X\ ,\ g.(h.x) = (gh).x$.

On omet en général le point dans la notation: $gx := g.x$ et l'on précise rarement "à gauche "[1].

L'application $G \to \mathcal{F}(X,X)$, qui, à $g \in G$, associe l'application $x \mapsto gx$ de X dans lui-même, envoie G dans le groupe $\mathfrak{S}(X)$ des permutations de X et c'est un morphisme de groupes $G \to \mathfrak{S}(X)$. Réciproquement, tout morphisme de groupes $\phi : G \to \mathfrak{S}(X)$ définit une action à gauche de G sur X par la formule $g.x := \phi(g)(x)$.

Exercice 1.1.2 Vérifier soigneusement le passage de la notion d'action telle que formulée dans la définition à celle de morphisme $G \to \mathfrak{S}(X)$ ainsi que le passage réciproque.

Exemples 1.1.3

1. G agit sur lui-même par la formule $g.h := gh$, où le membre gauche de l'égalité dénote l'effet de l'action de $g \in G$ sur $h \in X := G$ et le membre droit dénote le produit de g et h dans G. On parle d'*action par translations*. Notant L_g la translation $h \mapsto gh$ (la lettre L est pour "left ", sorry folks), on vérifie que $L_{gh} = L_g L_h$ et l'on a bien un morphisme $g \mapsto L_g$ de G dans $\mathfrak{S}(G)$. Ce morphisme est clairement injectif (car $L_g = \mathrm{Id}_G$ entraîne évidemment $g = 1$) et permet d'identifier G à un sous-groupe de $\mathfrak{S}(G)$; en particulier, si G est fini d'ordre n, il s'identifie à un sous-groupe de $\mathfrak{S}_n$ (théorème de Cayley).

[1] Une action *à droite* serait plutôt notée x^g et satisferait l'axiome $(x^g)^h = x^{gh}$. Elle donnerait lieu à un *anti-morphisme* $G \to \mathfrak{S}(X)$.

2. G agit également sur lui-même par la formule $g.h := ghg^{-1}$: *action par conjugaison*[2]. On vérifiera qu'en notant I_g l'*automorphisme intérieur* $h \mapsto ghg^{-1}$ de G, on a bien un morphisme $g \mapsto I_g$ de G dans $\mathfrak{S}(G)$. Le noyau de ce morphisme est le centre $Z(G)$ de G. Cette action de G sur lui-même ainsi que la précédente jouent un rôle important en théorie des groupes.

3. Le groupe symétrique $\mathfrak{S}(X)$ agit sur l'ensemble X par la formule $\sigma.x := \sigma(x)$. Le morphisme associé est l'identité de $\mathfrak{S}(X)$. En particulier, $\mathfrak{S}_n$ agit sur $\{1,\ldots,n\}$. Par restriction évidente, tout sous-groupe de $\mathfrak{S}_n$ agit sur $\{1,\ldots,n\}$: par exemple, si $\sigma \in \mathfrak{S}_n$, le sous-groupe $<\sigma>$ engendré par σ. Cette action a déjà implicitement été rencontrée dans l'étude de $\mathfrak{S}_n$; l'étude de ses "orbites " (voir plus loin) permet de trouver la décomposition de σ en cycles.

4. Soit K un corps commutatif. Le groupe linéaire $\mathrm{GL}_n(K)$ agit sur l'ensemble $\mathrm{Mat}_n(K)$ par la formule $P.M := PMP^{-1}$, menant à l' étude de la *similitude* des matrices carrées.

Exercice 1.1.4 Le groupe produit $\mathrm{GL}_n(K) \times \mathrm{GL}_p(K)$ agit sur l'ensemble $\mathrm{Mat}_{n,p}(K)$ par la formule $(P,Q).M := PMQ^{-1}$. (Cette action mène à l'étude de l'*équivalence* des matrices rectangulaires.)

Vocabulaire

Dans tout ce qui suit, le groupe G agit (à gauche) sur l'ensemble X.

L'*orbite* de $x \in X$, notée Gx ou $O(x)$, est l'ensemble des images de x sous l'action:

$$O(x) = Gx := \{gx \mid g \in G\}.$$

On vérifie facilement que la relation $x \sim y \underset{def}{\Leftrightarrow} \exists g \in G \ : \ y = gx$ est une relation d'équivalence sur X et que $O(x)$ est la classe de x. Les orbites forment donc une partition de X, d'où, quand X est fini, la formule:

$$|X| = \sum_{x \text{ modulo } G} |O(x)|.$$

La sommation "modulo G " signifie que l'on prend un représentant dans chaque classe (chaque orbite); elle n'a de sens que si le terme sommé ne dépend que de la classe de x modulo G.

Le *stabilisateur* de $x \in X$ est l'ensemble des éléments de G qui fixent x:

$$S_x := \{g \in G \mid gx = x\}.$$

On vérifie immédiatement que c'est un sous-groupe de G, en général non distingué. Il est clair que, $x \in X$ étant fixé, l'application $g \mapsto gx$ est surjective de G sur $O(x)$ et que $g, g' \in G$ ont même image si, et seulement si, $g^{-1}g'x = x$, *i.e.* $g^{-1}g' \in S_x$, *i.e.* $gS_x = g'S_x$. Elle induit donc une application bijective de l'ensemble quotient G/S_x (ensemble des classes à gauche gS_x) sur $O(x)$. En particulier, si le groupe G est fini, on a:

$$|O(x)| = |G/S_x| = [G : S_x] \ \text{ (indice dans } G \text{ du sous-groupe } S_x).$$

[2] Attention ! La formule $g^{-1}hg$ définirait une action à droite.

On a l'égalité:

$$S_{gx} = gS_xg^{-1}$$

en vertu du calcul suivant:

$$h \in S_{gx} \Longleftrightarrow hgx = gx \Longleftrightarrow g^{-1}hgx = x \Longleftrightarrow g^{-1}hg \in S_x \Longleftrightarrow h \in gS_xg^{-1}.$$

En particulier, les stabilisateurs de x et gx étant conjugués, ils ont même ordre (s'ils sont finis) et donc $|S_x|$ ne dépend que de la classe (l'orbite) de x. Ceci donne un sens à la formule suivante, qui découle immédiatement des deux précédentes; si l'on suppose G et X finis:

$$|X| = \sum_{x \text{ modulo } G} |G/S_x| = \sum_{x \text{ modulo } G} [G : S_x] = \sum_{x \text{ modulo } G} \frac{|G|}{|S_x|}.$$

C'est la *formule des orbites*.

La formule des classes

On fait agir G sur lui-même par conjugaison. L'orbite de $x \in G$ est sa *classe de conjugaison*, notée $C(x)$. Le stabilisateur de x est son normalisateur[3] $N(x)$. Les formules établies plus haut se spécialisent en $|C(x)| = [G : N(x)]$ et en la *formule des classes*:

Théorème 1.1.5 (Formule des classes)

$$|G| = \sum_{x \text{ modulo } G} [G : N(x)] = \sum_{x \text{ modulo } G} \frac{|G|}{|N(x)|}.$$

En pratique, on met souvent à part les éléments qui sont seuls dans leur classe; notant que:

$$N(x) = \{x\} \Longleftrightarrow x \in Z(G),$$

on a donc:

Corollaire 1.1.6

$$|G| = |Z(G)| + \sum_{\substack{x \text{ modulo } G \\ x \notin Z(G)}} [G : N(x)] = |Z(G)| + \sum_{\substack{x \text{ modulo } G \\ x \notin Z(G)}} \frac{|G|}{|N(x)|}.$$

Les termes $\dfrac{|G|}{|N(x)|}$ *sont des diviseurs non triviaux de* $|G|$.

On abrégera parfois $\sum_{\substack{x \text{ modulo } G \\ x \notin Z(G)}}$ en $\sum'$.

[3] Le *normalisateur* d'une partie X de G est par définition $N(X) := \{g \in G \mid gXg^{-1} = X\}$. Son *centralisateur* est $Z(X) := \{g \in G \mid \forall x \in X\ ,\ gx = xg\}$. Si $X = \{x\}$, ils sont égaux et on note $N(x)$ ou $Z(x)$. À l'opposé, $N(G) = G$ et $Z(G)$ est le centre de G.

Vocabulaire complémentaire

On revient à G agissant sur X.

L'action est *transitive* s'il y a une seule orbite. Dans ce cas, tous les stabilisateurs sont conjugués et l'on a (si G est fini) $|X| = [G : S_x]$ pour l'un quelconque d'entre eux.

Le *noyau* de l'action est l'ensemble des éléments de G agissant trivialement, autrement dit, le noyau de $G \to \mathfrak{S}(X)$ (donc un sous-groupe distingué de G). L'action est dite *fidèle* si son noyau est trivial.

Exemple 1.1.7 L'action de $\mathfrak{S}(X)$ sur X est libre et fidèle.

L'action est *libre* si tous les stabilisateurs sont triviaux. Elle est *librement transitive* si elle est libre et transitive. Dans ce cas, quel que soit $x \in X$, l'application $g \mapsto gx$ est une bijection de G sur X. On dit alors que X est un *espace homogène* ou un *torseur* sous (l'action de) G.

Exemple 1.1.8 Soit E un espace affine d'espace sous-jacent V. L'action par translations de V sur E est librement transitive.

Exercice 1.1.9 Définir l'action de $\mathrm{GL}(V)$ sur l'ensemble des bases de V et la qualifier.

1.2 p-groupes

Dans toute cette section, p désigne un nombre premier.

Définition 1.2.1 Un *p-groupe* est un groupe fini d'ordre une puissance de p.

Bien entendu, les sous-groupes et les groupes quotients d'un p-groupe sont des p-groupes.

Exemples 1.2.2 Soit $|G| = p^r$, $r \in \mathbf{N}$. Si $r = 0$, G est trivial. Si $r = 1$, G est cyclique d'ordre p, donc isomorphe à $\mathbf{Z}/p\mathbf{Z}$. Si $r = 2$, nous verrons que G est commutatif; il est alors isomorphe soit à $\mathbf{Z}/p^2\mathbf{Z}$ soit à $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ (*cf.* la classification des groupes abéliens finis vue en L3; on la reverra comme application de la troisième partie de ce cours). Si $r = 3$ et que G est commutatif, il y a trois structures possibles (d'après la même classification); mais G peut être non commutatif (on en verra des exemples avec $p = 2$).

Exercice 1.2.3 Vérifier l'assertion concernant le cas abélien.

On rappelle que l'*exposant* $e(G)$ d'un groupe fini G est le ppcm des ordres de ses éléments; c'est également le plus petit entier non nul k tel que $\forall x \in G$, $x^k = 1$. Puisque l'ordre de tout élément de G divise l'ordre de G (Lagrange), il est clair que l'exposant d'un p-groupe est une puissance de p. Nous verrons plus loin (corollaire au théorème de Cauchy) que la réciproque est vraie.

Proposition 1.2.4 *Soit G un p-groupe non trivial. Alors son centre $Z(G)$ est non trivial.*

Preuve. - On écrit la formule des classes sous la forme:

$$|Z(G)| = |G| - \sum_{\substack{x \text{ modulo } G \\ x \notin Z(G)}} \frac{|G|}{|N(x)|}.$$

Tous les termes du second membre sont des diviseurs non triviaux de $|G|$, donc des puissances non triviales de p, donc des multiples de p. Il en est donc de même de $|Z(G)|$, qui n'est donc pas égal à 1. □

Le centre $Z(G)$ est donc un p-groupe commutatif non trivial et le quotient $G/Z(G)$ (qui existe puisque le centre est distingué) est un p-groupe.

Corollaire 1.2.5 *Tout p-groupe est* résoluble*, autrement dit, on peut trouver une tour de sous-groupes $\{1\} = G_0 \subset \cdots \subset G_k = G$ telle que chaque G_i soit un sous-groupe distingué de G_{i+1} et que chaque G_{i+1}/G_i soit abélien.*

En fait, on peut même exiger que chaque G_{i+1}/G_i soit isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

Théorème 1.2.6 (Cauchy) *Soit G un groupe d'ordre n multiple de p. Alors il y a dans G des éléments d'ordre p.*

Preuve. - Le cas où G est abélien, qui se déduit immédiatement du cours de L3: G est alors isomorphe à un produit $\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_k\mathbf{Z}$, l'un des n_i, mettons n_1, est multiple de p (car $\prod n_i = n$); notant $m := n_1/p$ et $\overline{m}$ sa classe dans $\mathbf{Z}/n_1\mathbf{Z}$, on voit que l'élément $(\overline{m}, 0, \ldots, 0)$ convient.
La démonstration procède ensuite par récurrence forte sur n. Si $n = p$, la conclusion vient immédiatement. Supposons donc $n > p$.
Si $Z(G) = G$, on est dans le cas abélien. Sinon, soit $x \notin Z(G)$, de sorte que $N(x) \neq G$. Si $|N(x)|$ est multiple de p, par hypothèse de récurrence $N(x)$ admet des éléments d'ordre p donc G aussi.
On est donc ramené au cas où pour tout $x \notin Z(G)$ l'entier $|N(x)|$ est non multiple de p; mais cet entier divise $|G|$ qui l'est, le quotient $[G : N(x)]$ est donc multiple de p. De la formule des classes

$$|Z(G)| = |G| - \sum_{\substack{x \text{ modulo } G \\ x \notin Z(G)}} \frac{|G|}{|N(x)|},$$

on déduit que $|Z(G)|$ est multiple de p; du cas abélien on déduit enseuite que $Z(G)$ contient des éléments d'ordre p, donc G aussi. □

Une autre démonstration est proposée en exercice.

Corollaire 1.2.7 *Pour que le groupe fini G soit un p-groupe, il faut, et il suffit, que son exposant soit une puissance de G.*

Preuve. - On a déjà vu que c'était nécessaire. Prouvons la suffisance par contraposition. Si G n'est pas un p-groupe, un nombre premier $q \neq p$ divise son ordre, il y a donc des élements d'ordre q et l'exposant est multiple de q donc n'est pas une puissance de p. □

Exemples 1.2.8 1. Si $|G| = p^2$, $|Z(G)| = p$ ou p^2. Dans le premier cas, si $a \in G \setminus Z(G)$, le sous-groupe engendré par $Z(G)$ et a est égal à G et il est abélien. Le premier cas est donc impossible et G est certainement abélien.

2. Si $|G| = p^3$, $|Z(G)| = p$ ou p^2 ou p^3. Le deuxième cas est impossible (même argument que ci-dessus). Le troisième cas est celui où G est abélien, il y a alors trois structures possibles: $\mathbf{Z}/p^3\mathbf{Z}$, $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p^2\mathbf{Z}$ et $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$. Donc si G n'est pas commutatif, $|Z(G)| = p$. Il y a plusieurs structures possibles, voir par exemple Lang (ou encore le livre "An Introduction to the Theory of Groups" de Rotman).

3. Si $|G| = 8$ et G non abélien, son centre a deux éléments. Il n'y a pas d'élément d'ordre 8 (sinon le groupe serait cyclique). Si tous les éléments étaient d'ordre 2, le groupe serait abélien. Il y a donc un élément a d'ordre 4. Soit $H := < a > = \{1, a, a^2, a^3\}$, qui est d'indice 2 donc distingué. Soit $b \in G \setminus H$. L'automorphisme intérieur I_b conserve H, donc induit un automorphisme de H, qui ne peut être l'identité (sinon $G = < a, b >$ serait commutatif) donc qui est l'application $x \mapsto x^{-1}$. Comme $b^2 \in H$ (car ce dernier est d'indice 2) et $(b^2)^2 = 1$ (car il n'y a pas d'élément d'ordre 8), on distingue alors deux cas:

   - $b^2 = 1$: on trouve alors que G est isomorphe au groupe diédral D_4 (qui se réalise par exemple comme groupe des isométries du carré);
   - $b^2 = a^2$: dans ce cas G est isomorphe au groupe de quaternions[4] $\{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$.

1.3 les théorèmes de Sylow

Dans toute cette section, p désigne un nombre premier et G un groupe fini d'ordre $n = p^\alpha m$, où $\alpha \geq 1$ et $p \not| m$.

Définition 1.3.1 Un *p-sous-groupe de Sylow* ou *p-Sylow* de G est un sous-groupe d'ordre p^α.

Théorème 1.3.2 (Sylow) *Le groupe G admet des p-Sylow.*

Preuve. - La démonstration se fait par récurrence forte sur l'ordre de G. Si $n = p$, c'est trivial, on suppose donc $n > p$. Si G admet un sous-groupe d'ordre $p^\alpha m'$, $m' < m$, ce dernier admet un p-Sylow (récurrence) qui est également un p-Sylow de G. Dans le cas contraire, tout sous-groupe propre de G est d'indice multiple de p. De la formule des classes, on déduit que $|Z(G)|$ est multiple de p, donc qu'il contient un élément a d'ordre p. Le groupe $H := < a >$ est central, donc distingué et le quotient G/H est d'ordre $p^{\alpha-1}m$. Si $\alpha = 1$, H lui-même est un p-Sylow. Sinon, par hypothèse de récurrence, G/H admet un p-Sylow, donc un sous-groupe d'ordre $p^{\alpha-1}$; ce sous-groupe est de la forme G'/H et G' est un p-Sylow de G. □

Il est évident que tout conjugué d'un p-Sylow est un p-Sylow et donc que G agit par conjugaison sur l'ensemble des p-Sylow. On va voir que cette action est transitive (point (ii) du théorème qui suit); le nombre de p-Sylow est donc le cardinal de l'unique orbite, donc l'indice du stabilisateur de l'un quelconque d'entre eux, c'est-à-dire l'indice de son normalisateur; donc, par calcul simple, un diviseur de m.

[4] Rappelons que le corps des quaternions est la $\mathbf{R}$-algèbre $\mathbf{H} := \mathbf{R} + \mathbf{Ri} + \mathbf{Rj} + \mathbf{Rk}$ caractérisée par les relations $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ et $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$, $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$ et $\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$.

Théorème 1.3.3 (Sylow) *(i) Tout p-sous-groupe de G (*i.e. *tout sous-groupe de G qui est un p-groupe) est inclus dans un p-Sylow.*
(ii) Les p-Sylow sont tous conjugués entre eux.
(iii) Le nombre de p-Sylow est congru à 1 modulo p (et il divise m d'après l'argument qui précède le théorème).

Preuve. - Soient H un p-sous-groupe et P un p-Sylow de G. On va montrer que H est inclus dans un conjugué de P, ce qui prouvera à la fois (i) et (ii). Pour cela, on note S l'ensemble des conjugués de P (son orbite). On a $|S| = [G : N(P)]$ et $N(P) \supset P$ a $p^\alpha m'$ éléments, où $m'|m$, donc $|S| = m/m'$; en particulier, $p \not| |S|$. On, fait agir H par conjugaison sur S. Les orbites de cette action ont des cardinaux divisant $|H|$ donc des puissances de p. Si toutes ces orbites étaient non triviales, leurs cardinaux seraient des multiples de p et donc $|S|$ également. Donc l'une des orbites est triviale, de la forme $\{P'\}$, où P' est un conjugué de P (donc un p-Sylow) tel que $\forall h \in H$, $hP'h^{-1} = P'$, c'est-à-dire $H \subset N(P')$. L'image de H dans $N(P')/P'$ est d'ordre une puissance de p (car cet ordre divise celui de H); mais l'ordre de $N(P')/P'$ est non multiple de P (même argument que précédemment). L'image de H dans $N(P')/P'$ est donc triviale, autrement dit $H \subset P'$, ce qui était le point à établir et d'où découlent (i) et (ii).
Pour prouver (iii), on prend $H = P$ dans l'argument ci-dessus. On sait que S est l'ensemble des p-Sylow (d'après (ii)) et que son cardinal est non multiple de P. L'unique orbite sous $H = P$ dont le cardinal ne soit pas un multiple de p est celle qui a un seul élément, c'est-à-dire $\{P\}$: on a donc bien $|S| \equiv 1 \pmod{p}$. □

Exemples 1.3.4

1. Dans $\mathfrak{S}_3$, il y a trois 2-Sylow, les $\{e, \tau\}$, où τ est une transposition; et un 3-Sylow $\{e, \sigma, \sigma^2\}$, où σ est l'un des deux 3-cycles (c'est le groupe alterné).

2. Le groupe linéaire sur $\mathbf{F}_p$ (p premier) est d'ordre

$$|\mathrm{GL}_n(\mathbf{F}_p)| = \prod_{i=0}^{n-1}(p^n - p^i) = p^{n(n-1)/2}\prod_{i=1}^{n}(p^i - 1).$$

   Le sous groupe formé des matrices triangulaires supérieures unipotentes est d'ordre $p^{n(n-1)/2}$, c'en est donc un p-Sylow.

3. Dans $\mathfrak{S}_4$, qui est d'ordre $24 = 8 \times 3$, il y a quatre 3-Sylow, les $\{e, \sigma, \sigma^2\}$, où σ est l'un des huit 3-cycles. D'après le théorème, le nombre des 2-Sylow est un diviseur de 3 impair; et tout élément d'ordre 1, 2, 4 ou 8 appartient à un 2-Sylow. Si le nombre de 2-Sylow était 1, l'unique 2-Sylow contiendrait toutes les transpositions, or celles-ci engendrent $\mathfrak{S}_4$. Donc il y a trois 2-Sylow. Ils contiennent tous le sous-groupe distingué $H := \{e, ((12)(34)), ((13)(24)), ((14)(23))\}$ et en fait chacun s'obtient en adjoignant à H deux transpositions et deux 4-cycles.

Exercice 1.3.5 Si G est abélien, il a un seul p-Sylow, qui est formé des éléments dont l'ordre est une puissance de p ("composante de p-torsion ", voir la troisième partie du cours).

1.4 Exercices sur le chapitre "Actions de groupes"

Première série

Exercice 1.4.1 (i) Soient G un groupe agissant sur un ensemble X et G' un sous-groupe de G. définir l'action de G' sur X et comparer les orbites des deux actions.
(ii) Application: $G := \mathfrak{S}_n$, $X := \{1,\dots,n\}$, $G' :=< \sigma >$ où $\sigma \in \mathfrak{S}_n$ est quelconque.

Exercice 1.4.2 (i) Écrire les axiomes de l'action à gauche d'un groupe noté additivement.
(ii) Soient p un nombre premier et G un groupe fini d'ordre n. On fait agir $\mathbf{Z}/p\mathbf{Z}$ sur $X := \{(x_1,\dots,x_p) \in G^p \mid x_1 \cdots x_p = e\}$ par $(\overline{1},(x_1,\dots,x_p)) \mapsto (x_2,\dots,x_p,x_1)$ (ce qui définit complètement l'action). Déterminer les orbites de cardinal 1, écrire la formule des orbites, et en déduire que, si $p|n$, alors G admet des éléments d'ordre p (deuxième preuve du théorème de Cauchy).

Exercice 1.4.3 Soit G un groupe fini d'ordre pq, où p, q sont premiers, $p < q$ et p ne divise pas $q-1$. On suppose G non commutatif[5].
(i) Appliquer les théorèmes de Sylow.
(ii) Soit K un sous-groupe distingué de G tel que G/K soit commutatif. Montrer que, quels que soient $x, y \in G$, leur commutateur $xyx^{-1}y^{-1}$ appartient à K.
(iii) Conclure.

Exercice 1.4.4 On fait agir $\mathrm{GL}_2(\mathbf{C})$ sur $\mathbf{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$ par la formule

$$\text{Si } g := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ alors } g.z := \frac{az+b}{cz+d}.$$

(i) Préciser les règles concernant les cas spéciaux $z = \infty$ et $cz+d = 0$, puis vérifier qu'on a bien une action à gauche. (Indication: identifier $\mathbf{P}^1(\mathbf{C})$ à l'ensemble des droites vectorielles de $\mathbf{C}^2$.)
(ii) Déterminer le noyau K de l'action et le groupe $\mathbf{P}\mathrm{GL}_2(\mathbf{C}) := \mathrm{GL}_2(\mathbf{C})/K$ (qui agit donc fidèlement sur $\mathbf{P}^1(\mathbf{C})$).
(iii) Montrer que l'action de $\mathrm{GL}_2(\mathbf{C})$ sur l'ensemble $\{(x,y,z) \in \mathbf{P}^1(\mathbf{C})^3 \mid x \neq y \neq z \neq x\}$ est transitive; on dit que l'action est 3-*transitive*. (Indication: déterminer une homographie telle que $0 \mapsto x$, $1 \mapsto y$, $\infty \mapsto z$.)

Deuxième série

Exercice 1.4.5 On reprend les notations de l'exercice précédent.
(i) Soient $g := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{R})$ et $z \in \mathbf{C} \setminus \mathbf{R}$. Vérifier que $g.z \in \mathbf{C} \setminus \mathbf{R}$.
(ii) Calculer $\mathrm{Im}(gz)$ en fonction de $\mathrm{Im}\, z$ et en déduire une action du *groupe modulaire* $\mathrm{SL}_2(\mathbf{R})$ sur le *demi-plan de Poincaré* $\mathcal{H} := \{z \in \mathbf{C} \mid \mathrm{Im}\, z > 0\}$.
(iii) Montrer que l'action est transitive. (Indication: déterminer l'orbite de i.)
(iv) Reconnaître le stabilisateur de i.

Exercice 1.4.6 Soit G un groupe non commutatif fini d'ordre pq, où p, q sont premiers et p divise $q-1$. Poursuivre aussi loin que possible l'étude de la structure de G. Donner un exemple.

[5] Si G est commutatif, il découle du cours de L3 sur les groupes abéliens finis qu'il est cyclique.

Chapter 2

Représentations linéaires

Dans ce chapitre, K désigne un corps commutatif. À partir de la section 2.4, le corps de base sera $\mathbf{C}$.

2.1 Définitions, vocabulaire, exemples

Définition 2.1.1 Une *représentation (linéaire)* du groupe G dans le K-espace vectoriel V est une action à gauche de G dans V telle que, pour tout $g \in G$, l'application $x \mapsto gx$ de V dans lui-même est linéaire. De manière équivalente, c'est un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$, le lien étant donné par la formule $\rho(g)(x) = gx$. Nous ne considérerons dans ce cours que des espaces vectoriels V de dimension finie. Le *degré* de la représentation est la dimension $\dim_K(V)$ de l'*espace sous-jacent* V.

Exercice 2.1.2 Vérifier soigneusement l'équivalence entre les deux définitions proposées.

Par choix d'une base de V, on identifie $\mathrm{GL}(V)$ à $\mathrm{GL}_n(K)$ (où n est le degré de la représentation).

Définition 2.1.3 Une *représentation matricielle de degré n* du groupe G est un morphisme de groupes $G \to \mathrm{GL}_n(K)$.

On peut également la considérer comme une représentation de G dans K^n.

Définition 2.1.4 Deux représentations $\rho_i : G \to \mathrm{GL}(V_i)$, $i = 1,2$ (donc d'un même groupe) sont dites *équivalentes* s'il existe un isomorphisme $u : V_1 \to V_2$ qui les "entrelace "(en anglais: "intertwines"):

$$\forall g \in G\ ,\ \rho_2(g) \circ u = u \circ \rho_1(g).$$

De manière équivalente, u est *équivariant*:

$$\forall g \in G\ ,\ \forall x \in V_1\ ,\ u(gx) = gu(x).$$

Deux représentations équivalentes ont donc même degré. Selon les mots de Serre, "on peut sans inconvénient identifier deux telles représentations ".

Le choix d'une base $\mathcal{B}$ de V définit un isomorphisme $u : K^n \to V$ qui entrelace une représentation de G dans V à la représentation matricielle correspondante.

Exercice 2.1.5 Deux représentations matricielles $\rho_i : G \to \mathrm{GL}_{n_i}(K)$, $i = 1,2$, sont équivalentes si $n_1 = n_2 =: n$ et s'il existe $P \in \mathrm{GL}_n(K)$ tel que:

$$\forall g \in G\ ,\ \rho_2(g) = P\rho_1(g)P^{-1}.$$

(P est donc indépendant de g.)

Exemples 2.1.6

1. La *représentation triviale* de G dans V est celle qui, à tout $g \in G$, associe Id_V (version matricielle: $g \mapsto I_n$). Quand on parle de *représentation triviale* de G sans préciser V, il est entendu que $V = \{0\}$.

2. La représentation naturelle de $\mathrm{GL}(V)$ dans V correspond au morphisme identité de $\mathrm{GL}(V)$. Elle induit la représentation naturelle de tout sous-groupe de $\mathrm{GL}(V)$ dans V.

3. L'action naturelle de $\mathfrak{S}_n$ dans K^n est une représentation. Vue comme représentation matricielle, elle envoie les éléments de $\mathfrak{S}_n$ sur les matrices de permutation.

4. L'action de $\mathfrak{S}_n$ sur $K[X_1,\ldots,X_n]$ (permutation des indéterminées) laisse stable le sous-espace $K[X_1,\ldots,X_n]_d$ des polynômes homogènes de degré d et définit une représentation de $\mathfrak{S}_n$ dans $K[X_1,\ldots,X_n]_d$. (Quel est son degré ?)

5. L'action de $\mathrm{GL}_n(K)$ sur $K[X_1,\ldots,X_n]$ (substitution linéaire des indéterminées) laisse stable $K[X_1,\ldots,X_n]_d$ et définit une représentation de $\mathrm{GL}_n(K)$.

6. Une représentation de $\mathbf{Z}$ dans V est entièrement définie par l'image de 1, c'est-à-dire par la donnée d'un automorphisme de V. Deux telles représentations sont équivalentes si, et seulement si, les automorphismes correspondants sont conjugués.

7. Une représentation de $\mathbf{Z}/m\mathbf{Z}$ dans V est entièrement définie par l'image de $\overline{1}$, c'est-à-dire par la donnée d'un automorphisme u de V tel que $u^m = \mathrm{Id}_V$.

8. Une représentation de $\mathbf{Z} \times \mathbf{Z}$ dans V est entièrement définie par les images de $(1,0)$ et de $(0,1)$, c'est-à-dire par la donnée de deux automorphismes de V qui commutent.

9. Le groupe $\mathfrak{S}_3$ est défini par des générateurs σ, τ (un 3-cycle et une transposition) soumis aux relations $\sigma^3 = e$, $\tau^2 = e$ et $\tau\sigma\tau = \sigma^{-1}$. Une représentation de $\mathfrak{S}_3$ dans V est entièrement définie par les images de σ et de τ, c'est-à-dire par la donnée de deux automorphismes u et v de V tels que $u^3 = v^2 = \mathrm{Id}_V$ et $vuv = u^{-1}$.

Définition 2.1.7 La *représentation régulière* du groupe fini G a pour espace sous-jacent un espace vectoriel V de base $(e_g)_{g\in G}$ (son degré est donc l'ordre de G), l'action étant définie par $h.e_g := e_{hg}$ (et étendue par linéarité). L'action est donc donnée par la formule:

$$h.\sum_{g\in G} \lambda_g e_g := \sum_{g\in G} \lambda_g e_{hg} = \sum_{g\in G} \lambda_{h^{-1}g} e_g.$$

On peut réaliser un tel espace V comme $\mathcal{F}(G,K)$ (applications de G dans K), avec $e_g : h \mapsto \delta_{g,h}$.

Exercice 2.1.8 Vérifier que l'action est alors donnée par la formule $h.f : x \mapsto f(h^{-1}x)$.

2.2 Représentations irréductibles

Définition 2.2.1 (i) Soit $\rho : G \to \mathrm{GL}(V)$ une représentation. Un sous-espace $W \subset V$ est dit *G-stable* si $gW = W$ pour tout $g \in G$. On définit ainsi une représentation $g \mapsto \rho(g)_{|W}$ de G dans W qui est une *sous-représentation* de ρ.
(ii) La représentation ρ est dite *irréductible* si elle est non nulle (*i.e.* de degré $\neq 0$) et si ses seules sous-représentations sont la représentation nulle et elle-même; autrement dit, si les seuls sous-espaces G-stables de V sont $\{0\}$ et V.

Exercice 2.2.2 Que dire de la condition plus générale $gW \subset W$?

Remarque 2.2.3 En choisissant une base de W et en l'étendant en une base de V, on voit que la représentation matricielle associée à ρ a pour images des matrices triangulaires par blocs:

$$\rho(g) = \begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix}.$$

Le bloc carré $A(g)$ est de taille $\dim_K W$, il correspond à la sous-représentation d'espace W. Le bloc $C(g)$ correspond à la "représentation quotient ", que nous n'étudierons pas.
Le bloc $B(g)$ peut être identiquement annulé si W admet un supplémentaire stable (on prend alors pour V une base adaptée à cette décomposition). Cette question sera creuséee à la section 2.3.

Définition 2.2.4 Soient $\rho_i : G \to \mathrm{GL}(V_i)$, $i = 1,2$, deux représentations. Une application linéaire $u : V_1 \to V_2$ est dite *équivariante* si:

$$\forall g \in G\ ,\ \rho_2(g) \circ u = u \circ \rho_1(g).$$

De manière équivalente:

$$\forall g \in G\ ,\ \forall x \in V_1\ ,\ u(gx) = gu(x).$$

Si u est bijective, on retrouve la notion de représentations équivalentes.

Lemme 2.2.5 *Soient $\rho_i : G \to GL(V_i)$, $i = 1,2$, deux représentations et soit $u : V_1 \to V_2$ une application linéaire équivariante. Alors Ker $u \subset V_1$ et Im $u \subset V_2$ sont G-stables.*

Preuve. - Laissée en exercice. □

Théorème 2.2.6 (Lemme de Schur) *Soient $\rho_i : G \to GL(V_i)$, $i = 1,2$, deux représentations irréductibles et soit $u : V_1 \to V_2$ une application linéaire équivariante.*
(i) Si ρ_1 et ρ_2 ne sont pas équivalentes, $u = 0$.
(ii) On suppose ici K algébriquement clos. Si $\rho_1 = \rho_2$ (donc $V_1 = V_2 =: V$) alors u est une homothétie.

Preuve. - (i) Si $u \neq 0$, Ker u est un sous-espace strict de V_1, stable d'après le lemme, donc nul (puisque ρ_1 est irréductible); et Im u est un sous-espace non nul de V_2, stable d'après le lemme, donc égal à V_2 (puisque ρ_2 est irréductible). L'application linéaire équivariante u est donc bijective et définit l'équivalence annoncée.
(ii) Soit λ une valeur propre de u (c'est ici qu'intervient l'hypothèse sur K). Alors $v := u - \lambda \mathrm{Id}_V$

est équivariante, son noyau est non nul et stable, son image est strictement incluse dans V et stable, donc $v = 0$. □

Remarque 2.2.7 La représentation de $G := \mathbf{Z}/4\mathbf{Z}$ dans $\mathbf{R}^2$ définie par $\overline{1} \mapsto A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est irréductible, l'application $A : \mathbf{R}^2 \to \mathbf{R}^2$ est équivariante mais n'est pas une homothétie.

2.3 Complète réductibilité

Lemme 2.3.1 *Soit $\rho : G \to GL(V)$ une représentation. Soit $W \subset V$ un sous-espace G-stable. Pour que W admette un supplémentaire stable, il faut, et il suffit, qu'il existe un projecteur p sur W qui soit équivariant,* i.e. $\forall g \in G\ ,\ \forall x \in V\ ,\ p(gx) = gp(x)$.

Preuve. - Soit p un tel projecteur. L'hypothèse dit que p commute à tous les $\rho(g)$. Ces derniers laissent donc stables les sous-espaces propres de p, c'est-à-dire $W = \mathrm{Im}p$ et son supplémentaire $\mathrm{Ker}\ p$.
Réciproquement, si W est un supplémentaire stable de V et si $x = v + w$ est une décomposition, alors $gx = gv + gw$ où $gv \in V$ et $gw \in W$. Alors $p(gx) = gv = gp(x)$. □

Théorème 2.3.2 (Maschke) *On suppose que G est fini d'ordre inversible dans K (autrement dit, non multiple de la caractéristique de K; c'est à coup sûr le cas si K est de caractéristique nulle). Alors tout sous-espace G-stable de V admet un supplémentaire stable.*

Preuve. - Soit W un sous-espace stable et soit p un projecteur arbitraire sur V. On pose:

$$p^0 := \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ p \circ \rho(g)^{-1}.$$

Si l'on fixe $g_0 \in G$, on calcule:

$$\begin{aligned} \rho(g_0) \circ p^0 \circ \rho(g_0)^{-1} &= \frac{1}{|G|} \sum_{g \in G} \rho(g_0) \circ \rho(g) \circ p \circ \rho(g)^{-1} \circ \rho(g_0)^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \rho(g_0 g) \circ p \circ \rho(g_0 g)^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ p \circ \rho(g)^{-1} = p^0. \end{aligned}$$

L'avant-dernière égalité vient de ce que $g \mapsto g_0 g$ est une permutation de G.
On voit donc déjà que p^0 est équivariant. L'image de chaque $p \circ \rho(g)^{-1}$ est dans W, donc également l'image de chaque $\rho(g) \circ p \circ \rho(g)^{-1}$ (puisque W est G-stable), donc, par linéarité, l'image de p^0. D'autre part, si $x \in W$, alors, pour tout $g \in G$:

$$g^{-1}x \in W \Longrightarrow p(g^{-1}x) = g^{-1}x \Longrightarrow gp(g^{-1}x) = x,$$

autrement dit, $\rho(g) \circ p \circ \rho(g)^{-1}(x) = x$. On a donc:

$$p^0(x) = \frac{1}{|G|} \sum_{g \in G} x = x,$$

ce qui finit d'établir que p^0 est un projecteur d'image W. Comme il est équivariant, on déduit du lemme que W admet un supplémentaire G-stable. □

Une autre preuve est proposée en exercice (valable lorsque le corps de base est $\mathbf{C}$). Dans un sens évident, on peut dire que ρ est *somme directe de deux sous-représentations*.

Corollaire 2.3.3 *Toute représentation non nulle de G est* complétement réductible, *c'est-à-dire somme directe de représentations irréductibles.*

Preuve. - C'est immédiat par récurrence forte sur le degré, en appliquant le théorème de Maschke. □

Remarque 2.3.4 (i) Soient $K := \mathbf{C}$ et $G := \mathbf{Z}$. La représentation de G dans $V := K^2$ telle que $1 \in G$ a pour image $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ admet pour seul sous-espace stable (autre que $\{0\}$ et V) la droite W de vecteur directeur $(1,0)$. Celle-ci n'admet donc pas de supplémentaire stable et la représentation n'est pas complétement réductible.
(ii) Soient $K := \mathbf{F}_2$ (le corps à 2 éléments) et $G := \mathbf{Z}/2\mathbf{Z}$. La représentation de G dans $V := K^2$ telle que $\overline{1} \in G$ a pour image $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ admet pour seul sous-espace stable (autre que $\{0\}$ et V) la droite W de vecteur directeur $(1,0)$. Celle-ci n'admet donc pas de supplémentaire stable et la représentation n'est pas complétement réductible.

Exercice 2.3.5 Où intervient la condition sur la caractéristique dans cet exemple ? Par exemple, pourquoi ne pas prendre $K := \mathbf{F}_p$ (corps à p éléments) et $G := \mathbf{Z}/q\mathbf{Z}$ avec p, q premiers distincts ?

2.4 Représentations des groupes abéliens finis

Pour tout le reste de ce chapitre, le corps de base est $K = \mathbf{C}$. Soit G un groupe abélien fini, d'ordre $|G| = n$.

Théorème 2.4.1 *Toute représentation de G est somme directe de représentations de degré* 1.

Preuve. - Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire de G. Pour tout $g \in G$, on a $g^n = e$ (Lagrange) donc $\rho(g)^n = \mathrm{Id}_V$. L'endomorphisme $\rho(g)$ étant annulé par le polynôme $X^n - 1$, qui est scindé à racines simples, il est diagonalisable. Pour tous $g, h \in G$, on a $gh = hg$ (hypothèse) donc $\rho(g)\rho(h) = \rho(h)\rho(g)$. Les endomorphismes diagonalisables $\rho(g)$ commutant deux à deux, ils sont codiagonalisables. Soit $(e_i)_{1 \le i \le d}$ une base de vecteurs propres communs ($d := \dim_K V$). Alors chaque droite $D_i := \mathbf{C}e_i$ est G-stable et $V = \bigoplus_{i=1}^{d} D_i$ est la décomposition annoncée. □

Corollaire 2.4.2 *Les représentations irréductibles de G sont les représentations de degré* 1.

On note alors que, pour tout espace vectoriel de degré 1, le groupe linéaire $\mathrm{GL}(V)$ s'identifie à $\mathbf{C}^*$ *canoniquement*, c'est-à-dire sans choix de base (tout endomorphisme d'une droite vectorielle est une homothétie). Une représentation de degré 1 s'identifie donc à un morphisme de G dans $\mathbf{C}^*$.

Définition 2.4.3 On appelle *caractère* de G un morphisme de G dans $\mathbf{C}^*$.

Cette définition correspond à ce qui sera appelé à la section suivante un *caractère irréductible*, mais elle est traditionnelle dans la théorie de la "dualité des groupes abéliens finis ".

Proposition 2.4.4 *En posant $(\chi\chi')(g) := \chi(g)\chi'(g)$, on munit l'ensemble $\hat{G}$ des caractères de G d'une structure de groupe abélien, le* dual *de G.*

Preuve. - La preuve est mécanique[1] et laissée au lecteur. □

Exemples 2.4.5
1. Le dual de $\mathbf{Z}/n\mathbf{Z}$ est μ_n (groupe des racines $n^{\text{èmes}}$ de l'unité).
2. Le dual d'un groupe produit $G = G_1 \times G_2$ s'identifie au groupe produit $\hat{G_1} \times \hat{G_2}$.

Exercice 2.4.6 Vérifier ces assertions.

Proposition 2.4.7 *Pour tout groupe fini G, le groupe dual $\hat{G}$ est isomorphe à G.*

Preuve. - Puisque μ_n est cyclique d'ordre n et puisque tout groupe abélien fini est produit de groupes cycliques, cela découle de ce qui précède. □

Attention ! Cet isomorphisme n'est pas canonique.

Lemme 2.4.8 *Soit $a \in G$, $a \neq 1$. Alors il existe $\chi \in \hat{G}$ tel que $\chi(a) \neq 1$.*

Preuve. - On peut, à isomorphisme près, supposer que $G = \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_k\mathbf{Z}$ et que $a = (\overline{a_1}, \ldots, \overline{a_k})$, avec $\overline{a_1} \neq 0$, *i.e.* $a_1 \not\equiv 0 \pmod{n_1}$. On définit alors χ par la formule $(\overline{x_1}, \ldots, \overline{x_k}) \mapsto e^{2i\pi x_1/n_1}$. □

Théorème 2.4.9 *L'application $x \mapsto (\chi \mapsto \chi(x))$ est un isomorphisme de G dans son bidual $\hat{\hat{G}}$.*

Preuve. - Le fait que ce soit bien défini et un morphisme est un argument classique de bidualité (le même que lorsqu'on définit l'application linéaire d'un espace vectoriel dans son bidual). Le fait qu'il soit injectif traduit le lemme qui précède. Comme les deux groupes ont même ordre (on sait déjà qu'ils sont isomorphes), c'est bien un isomorphisme. □

La nouveauté n'est pas l'isomorphie des deux groupes mais le fait qu'elle soit canonique et explicite.

Théorème 2.4.10 (Relations d'orthogonalité) *(i) Pour tout $\chi \in \hat{G}$,* $\displaystyle\sum_{x \in G} \chi(x) = \begin{cases} n \text{ si } \chi \text{ est trivial,} \\ 0 \text{ sinon.} \end{cases}$

(ii) Pour tout $x \in G$, $\displaystyle\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n \text{ si } x = 1, \\ 0 \text{ sinon.} \end{cases}$

[1] Mais non tautologique: voir le problème de Mathématiques générales de l'agrégation externe 2018.

Preuve. - Chacune des deux formules découle de l'autre grâce au théorème de bidualité mais nous les prouverons tout de même séparément.
(i) Si χ est trivial, on a $\chi(x) = 1$ pour tout $x \in G$ et le résultat est immédiat. Sinon, on fixe $x_0 \in G$ tel que $\chi(x_0) \neq 1$; de la bijectivité de $x \mapsto x_0 x$, on tire alors:

$$\sum_{x\in G} \chi(x) = \sum_{x\in G} \chi(x_0 x) = \sum_{x\in G} \chi(x_0)\chi(x) = \chi(x_0) \sum_{x\in G} \chi(x) \Longrightarrow (1-\chi(x_0)) \sum_{x\in G} \chi(x) = 0,$$

d'où la conclusion.
(ii) Si $x = 1$, on a $\chi(x) = 1$ pour tout $\chi \in \hat{G}$ et le résultat est immédiat. Sinon, on fixe $\chi_0 \in G$ tel que $\chi_0(x) \neq 1$ (c'est possible grâce au lemme vu plus haut); de la bijectivité de $\chi \mapsto \chi_0\chi$, on tire alors:

$$\sum_{\chi\in\hat{G}} \chi(x) = \sum_{\chi\in\hat{G}} (\chi_0\chi)(x) = \sum_{\chi\in\hat{G}} \chi_0(x)\chi(x) = \chi_0(x) \sum_{\chi\in\hat{G}} \chi(x) \Longrightarrow (1-\chi_0(x)) \sum_{\chi\in\hat{G}} \chi(x) = 0,$$

d'où la conclusion. □

On définit alors sur $\mathcal{F}(G, \mathbf{C})$ un produit hermitien en posant:

$$< f_1, f_2 >:= \frac{1}{n} \sum_{g\in G} \overline{f_1(g)} f_2(g).$$

C'est en fait l'unique produit hermitien pour lequel la base des $\sqrt{n}\, e_g$ (*cf.* à la fin de la section 2.1 la définition de la représentation régulière) est orthonormale.

Corollaire 2.4.11 (Relations d'orthogonalité) *Les caractères de G forment une famille orthonormale.*

Preuve. - Soient χ_1, χ_2 des caractères et posons $\chi := \chi_1^{-1}\chi_2$. Comme χ_1 est à valeur dans le groupe des complexes de module 1, on a $\chi_1^{-1} = \overline{\chi_1}$ et la relation (ii) du théorème donne:

$$< \chi_1, \chi_2 >= \begin{cases} 1 \text{ si } \chi_1 = \chi_2, \\ 0 \text{ sinon.} \end{cases}$$

Remarque 2.4.12 Les *fonctions centrales* sont les $f \in \mathcal{F}(G, \mathbf{C})$ telles que $\forall g, h \in G\,,\ f(ghg^{-1}) = f(h)$: par exemple les caractères. Elles forment un sous-espace vectoriel de $\mathcal{F}(G, \mathbf{C})$. On verra plus loin que les caractères en forment une base orthonormée.

2.5 Théorie des caractères

Dans cette section, G est un groupe fini d'ordre n, non nécessairement abélien. Comme dans la section précédente, le corps de base est $\mathbf{C}$.

Définition 2.5.1 Le *caractère* d'une représentation $\rho : G \to \mathrm{GL}(V)$ est l'application $\chi_\rho : G \to \mathbf{C}$, $g \mapsto \mathrm{Tr}\, \rho(g)$.

Exemples 2.5.2 1. Le caractère de la représentation régulière est l'application $g \mapsto \begin{cases} n \text{ si } g = 1, \\ 0 \text{ sinon.} \end{cases}$

2. Le caractère d'une représentation triviale de degré d est l'application constante de valeur d.

3. Le caractère de la représentation naturelle de $\mathfrak{S}_n$ dans $\mathbf{C}^n$ est l'application $\sigma \mapsto |Fix(\sigma)|$ (nombre de points fixes de σ).

Il est clair que deux représentations équivalentes ont même caractère (car deux endomorphismes conjugués ont même trace). Le miracle est que la réciproque est vraie: nous démontrerons que *le caractère d'une représentation détermine celle-ci à isomorphisme près*. On peut donc sans ambiguïté parler de degré d'un caractère, de caractère irréductible, etc.

Proposition 2.5.3 *Soit χ_ρ un caractère de G.*
(i) χ_ρ est une fonction centrale.
(ii) $\chi_\rho(1) = d$ (degré de la représentation ρ).
(iii) $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.

Preuve. - Seule la dernière assertion est non triviale. Comme chaque $\rho(g)$ est d'ordre fini, ses valeurs propres sont racines de l'unité, donc de module 1, donc vérifient $\lambda^{-1} = \overline{\lambda}$. En les sommant on obtient la formule. □

Relations d'orthogonalité

On munit encore le $\mathbf{C}$-espace vectoriel $\mathcal{F}(G, \mathbf{C})$ du produit hermitien:

$$< f_1, f_2 >:= \frac{1}{n} \sum_{g \in G} \overline{f_1(g)} f_2(g).$$

Théorème 2.5.4 *Soient ρ_1, ρ_2 deux représentations irréductibles de G et soient χ_1, χ_2 leurs caractères respectifs. Alors:*

$$< \chi_1, \chi_2 >= \begin{cases} 1 \text{ si } \rho_1, \rho_2 \text{ sont équivalentes,} \\ 0 \text{ sinon.} \end{cases}$$

Preuve. - Il y a une preuve matricielle dans le livre de Serre, nous allons en donner une plus intrinsèque (mais pas nécessairement plus claire). Elle consiste en une suite de définitions et de petits lemmes d'algèbre linéaire dont la démonstration sera laissée au lecteur.

1. Soient $\rho_i : G \to \mathrm{GL}(V_i)$, $i = 1, 2$ deux représentations et soit $\phi : V_1 \to V_2$ une application linéaire quelconque. Alors:

$$\phi^0 := \frac{1}{n} \sum_{g \in G} \rho_2(g) \circ \phi \circ \rho_1(g)^{-1}$$

est une application linéaire équivariante de V_1 dans V_2, *i.e.* elle vérifie $\phi^0(gx) = g\phi^0(x)$ pour $g \in G$, $x \in V_1$. Il découle alors du lemme de Schur que, si ρ_1 et ρ_2 ne sont pas équivalentes, $\phi^0 = 0$; et si $\rho_1 = \rho_2 =: \rho$, c'est une homothétie. Notant (dans ce dernier cas) d le degré de ρ, le rapport de cette homothétie est égal à sa trace divisée par d, donc à $\frac{1}{d}\mathrm{Tr}(\phi)$ par un petit calcul facile.

2. Soient V, W deux espaces vectoriels. Soient $y \in W$ et $\lambda \in V^*$ (dual de V). On définit[2] une application linéaire $\lambda \otimes y : V \to W$ par la formule:

$$(\lambda \otimes y)(x) := \lambda(x)y.$$

Dans le cas où $V = W$, on a $\mathrm{Tr}(\lambda \otimes y) = \lambda(y)$ (pour le voir, si $y \neq 0$, le compléter en une base et exprimer λ dans la base duale).

3. Avec les notations ci-dessus, prenons pour V, W les espaces sous-jacents de deux représentations ρ_V et ρ_W. Nous noterons χ_V et χ_W les caractères correspondants. On a alors:

$$(\lambda \otimes y)^0(x) = \frac{1}{n} \sum_{g \in G} \lambda(g^{-1}x)(gy).$$

4. En particulier, si V et W sont irréductibles non isomorphes et si $x \in V$, $y \in W$, $\lambda \in V^*$ et $\mu \in W^*$:

$$\sum_{g \in G} \lambda(g^{-1}x)\mu(gy) = 0.$$

5. Si au contraire $V = W$, notant d leur degré:

$$\sum_{g \in G} \lambda(g^{-1}x)\mu(gy) = \frac{n}{d}\lambda(y)\mu(x).$$

6. Soient ϕ un endomorphisme de V, $(e_i)_{1 \leq i \leq d}$ une base de V et $(e_i^*)_{1 \leq i \leq d}$ la base duale de V^*. Alors:

$$\mathrm{Tr}\ \phi = \sum_{1 \leq i \leq d} e_i^*(\phi(e_i)).$$

7. Dans la formule 4 ci-dessus, faisons parcourir à x une base (e_i) de V, à y une base (f_j) de W, à λ la base duale (e_i^*) et à μ la base duale (f_j^*) et sommons. On trouve, en vertu de la formule 6:

$$\sum_{g \in G} \chi_V(g^{-1})\chi_W(g) = 0.$$

8. Dans la formule 5 ci-dessus, faisons parcourir à x et y une base (e_i) de V, et à λ et μ la base duale (e_i^*) et sommons. On trouve, en vertu de la formule 6:

$$\sum_{g \in G} \chi_V(g^{-1})\chi_V(g) = n.$$

Rappelons (proposition 2.5.3) que $\chi_V(g^{-1}) = \overline{\chi_V(g)}$: les deux dernières formules sont donc les relations d'orthogonalité voulues. □

[2] La notation vient de la théorie du "produit tensoriel ", elle est liée à l'isomorphisme (valable en dimension finie) $V^* \otimes W \simeq \mathcal{L}(V,W)$.

Applications à la réduction des représentations

Si deux représentations sont équivalentes, l'une est irréductible si, et seulement si, l'autre l'est. On appelle *type* une classe d'équivalence de représentations irréductibles. Ce sont les briques de base dans la constitution des représentations (un peu comme les nombres premiers parmi les entiers naturels). On va démontrer que cette décomposition (dont l'existence découle du théorème de Maschke) est essentiellement unique et qu'elle est entièrement déterminée par les propriétés des caractères. Il s'agit encore d'une suite de faits qui découlent simplement les uns des autres (pourvu qu'on les formule dans l'ordre adéquat). Nous nous contentons donc d'esquisser les arguments.

Pour simplifier les formulations, nous choisissons dans chaque type α un représentant $\rho_\alpha : G \to \mathrm{GL}(V_\alpha)$, de degré d_α, et nous notons χ_α son caractère.

1. Écrivons de manière abusive mais simplifiée $V = W_1 \oplus \cdots \oplus W_k$ une décomposition de la représentation $\rho : G \to \mathrm{GL}(V)$, de degré d et de caractère χ, en somme directe de représentations irréductibles $\rho_i : G \to \mathrm{GL}(W_i)$. Les caractères χ_i des ρ_i vérifient $\chi = \chi_1 + \cdots + \chi_k$ (additivité de la trace relativement à la somme directe des endomorphismes).

2. Pour les raisonnements et les calculs qui vont suivre, il est commode de regrouper les sous-représentations W_i par type. Notant n_α le nombre des W_i qui sont isomorphes à un V_α donné, on a donc:
$$V \simeq \bigoplus_\alpha V_\alpha^{n_\alpha} \Longrightarrow \chi = \sum_\alpha n_\alpha \chi_\alpha \text{ et } d = \sum_\alpha n_\alpha d_\alpha.$$
Ces formules ont un sens car les n_α sont presque tous nuls.

3. De l'égalité $\chi = \sum n_\alpha \chi_\alpha$ et des relations d'orthogonalité, on déduit, en faisant le produit scalaire avec un χ_α fixé:
$$n_\alpha = < \chi, \chi_\alpha > .$$
On en déduit que *la connaissance du caractère χ détermine complètement les n_α et donc la classe d'isomorphie de ρ*; dit autrement: *deux représentations ayant même caractère sont équivalentes.*

4. On en déduit également que la décomposition de V est "essentiellement " unique (au sens où les types qui y figurent et leurs multiplicités le sont).

5. On a $< \chi, \chi >= \sum n_\alpha^2$, qui est égal à 1 si, et seulement si, l'un des n_α vaut 1 et les autres 0. On en déduit que ρ *est irréductible si, et seulement si,* $< \chi, \chi >= 1$.

Exemple 2.5.5 Le groupe $\mathfrak{S}_3$ a deux représentations de degré 1, la représentation triviale et la signature.
La représentation naturelle dans $\mathbf{C}^3$ a une droite fixe D portée par $e_1+e_2+e_3$ (en notant (e_1, e_2, e_3) la base canonique). Le caractère correspondant est donc le caractère trivial.
Le produit hermitien naturel sur $\mathbf{C}^3$ est $\mathfrak{S}_3$-invariant, l'orthogonal de D est donc une sous-représentation de degré 2. On vérifie qu'elle est irréductible (car la seule droite $\mathfrak{S}$-stable de $\mathbf{C}^3$ et D) puis, en l'écrivant dans une base (par exemple $(e_1 - e_2, e_2 - e_3)$) que son caractère vérifie $\mathrm{Id} \mapsto 2$, $\tau \mapsto 0$ pour toute transposition et $\sigma \mapsto -1$ pour tout 3-cycle.
Il découlera soit de la décomposition de la représentation régulière (voir l'exercice 2.6.8) soit du lien avec les fonctions centrales (voir ci-dessous) que l'on a trouvé tous les caractères irréductibles

de $\mathfrak{S}_3$. On peut présenter leur table comme suit; on note χ_0 le caractère trivial, ε la signature et χ_2 le caractère irréductible de degré 2; et l'on appelle τ_i les trois transpositions et σ_j les deux 3-cycles:

	Id	τ_1	τ_2	τ_3	σ_1	σ_2
χ_0	1	1	1	1	1	1
ε	1	-1	-1	-1	1	1
χ_2	2	0	0	0	-1	-1

Exercice 2.5.6 Retrouver dans cet exemple les relations d'orthogonalité.

Fonctions centrales

Définition 2.5.7 L'espace des *fonctions centrales sur G* est le sous-espace de $\mathcal{F}(G,\mathbf{C})$ défini par:

$$Z(G,\mathbf{C}) := \{f \in \mathcal{F}(G,\mathbf{C}) \mid \forall g,h \in G\ ,\ f(ghg^{-1}) = f(h)\}.$$

Les caractères sont des fonctions centrales et il résulte des relations d'orthogonalité que les caractères irréductibles en forment un système orthonormal.

Théorème 2.5.8 *Les caractères irréductibles constituent une base (orthonormée) de* $Z(G,\mathbf{C})$.

Preuve. - Soit ϕ une fonction centrale. On va prouver que, si ϕ est orthogonale à tous les caractères irréductibles, alors elle est nulle. Nous aurons l'usage de la remarque suivante: si ρ est une représentation matricielle irréductible, alors $\overline{\rho} : g \mapsto \overline{\rho(g)}$ est également une représentation matricielle irréductible. Il en découle que, si χ est un caractère irréductible, alors $\overline{\chi}$ aussi.

Lemme 2.5.9 *Soient* ϕ *une fonction centrale et* $\rho : G \to GL(V)$ *une représentation irréductible de degré* d *et de caractère* χ. *Alors:*

$$\forall x \in V\ ,\ \sum_{g\in G} \phi(g)(gx) = \frac{n}{d} < \overline{\chi}, \phi > x.$$

Preuve. - Posons $\Phi := \sum_{g\in G} \phi(g)\rho(g) \in \mathcal{L}(V)$. Alors, pour tout $g_0 \in G$ fixé:

$$\rho(g_0)\Phi\rho(g_0)^{-1} = \sum_{g\in G} \phi(g)\rho(g_0)\rho(g)\rho(g_0)^{-1} = \sum_{g\in G} \phi(g)\rho(g_0 g g_0^{-1}) = \sum_{g\in G} \phi(g_0^{-1} g g_0)\rho(g) = \Phi,$$

car $g \mapsto g_0 g g_0^{-1}$ est une permutation de G et ϕ est centrale. De l'égalité $\rho(g_0)\Phi\rho(g_0)^{-1} = \Phi$ on déduit que Φ est équivariante, donc, d'après le lemme de Schur, que c'est une homothétie de rapport:

$$\frac{1}{d}\mathrm{Tr}\Phi = \frac{1}{d}\sum_{g\in G} \phi(g)\mathrm{Tr}\rho(g) = \frac{1}{d}\sum_{g\in G} \phi(g)\chi(g) = \frac{n}{d} < \overline{\chi}, \phi > .$$

La formule en découle immédiatement. □

Reprenons la preuve du théorème. Si ϕ est orthogonale à tous les caractères irréductibles, on a $\sum_{g\in G} \phi(g)(gx) = 0$ dans la formule ci-dessus. C'est vrai pour toute représentation irréductible, donc pour toute représentation d'après la complète réductibilité. On l'applique à la représentation

régulière avec $x = e_1$, donc $gx = e_g$. On obtient l'égalité $\sum_{g\in G} \phi(g)e_g = 0$, d'où, puisque les e_g sont linéairement indépendants, $\phi = 0$. □

Corollaire 2.5.10 *Le nombre de caractères irréductibles distincs de G est égal au nombre de ses classes de conjugaison.*

Preuve. - Notons temporairement C l'ensemble des classes de conjugaison de G. L'application de $\mathbf{C}^C$ dans $\mathcal{F}(G,\mathbf{C})$ qui, à $(x_c)_{c\in C}$ associe la fonction $\phi : G \to \mathbf{C}$ qui prend la valeur x_c sur c, induit un isomorphisme de $\mathbf{C}^C$ sur $Z(G,\mathbf{C})$, d'où l'égalité $\dim_{\mathbf{C}} Z(G,\mathbf{C}) = |C|$; mais cette dimension est aussi le cardinal de la base formée des caractères irréductibles. □

Exemples 2.5.11 Sur un groupe abélien d'ordre n, il y a n caractères irréductibles: c'est bien l'ordre de $\hat{G}$. Sur $\mathfrak{S}_3$ et $\mathfrak{S}_4$, il y a respectivement 3 et 5 caractères irréductibles.

2.6 Exercices sur le chapitre "Représentations linéaires "

Première série

Exercice 2.6.1 Décrire matriciellement l'action de $\mathrm{GL}_2(K)$ sur $K[X,Y]_2$ et son caractère.

Exercice 2.6.2 (i) Soit $\rho : G \to \mathrm{GL}(V)$ une représentation complexe de dimension finie d'un groupe fini G. Soit $< -,- >$ un produit hermitien quelconque sur V. Montrer qu'en posant:

$$(x,y) := \sum_{g\in G} < gx, gy >,$$

on définit un produit hermitien sur V et que celui-ci est *G-invariant*, autrement dit:

$$\forall x,y \in V \ , \ \forall g \in G \ , \ (gx,gy) = (x,y).$$

(ii) Soit $W \subset V$ un sous-espace stable. Montrer que l'orthogonal de W (au sens du produit hermitien invariant) est stable. En déduire une nouvelle preuve du théorème de Maschke.

Exercice 2.6.3 Soit $\rho : G \to \mathrm{GL}(V)$ une représentation complexe irréductible du groupe abélien G. Vérifier que chaque $\rho(g_0) : V \to V$, $g_0 \in G$, est équivariant. Que dit alors le lemme de Schur ?

Exercice 2.6.4 Vérifier les assertions concernant la représentation irréductible de degré 2 dans l'exemple 2.5.5.

Exercice 2.6.5 (i) Vérifier qu'il y a 5 classes de conjugaison dans $\mathfrak{S}_4$. (Indication: utiliser le critère de conjugaison dans $\mathfrak{S}_n$ portant sur la décomposition en cycles.)
(ii) Décomposer la représentation naturelle de $\mathfrak{S}_4$ dans $\mathbf{C}^4$ en somme directe de représentations irréductibles, puis dresser la table des caractères irréductibles de $\mathfrak{S}_4$.

Deuxième série

Exercice 2.6.6 Décrire les représentations irréductibles des deux groupes non commutatifs d'ordre 8 et leurs caractères.

Exercice 2.6.7 On reprend les notations de l'exercice 2.6.2. Prenant pour G un sous-groupe de $\mathrm{GL}(V)$ et pour ρ l'inclusion, montrer que G est inclus dans le groupe unitaire de l'espace hermitien V (muni du produit hermitien $(-,-)$). En déduire que tout sous-groupe fini de $\mathrm{GL}_n(\mathbf{C})$ est conjugué à un sous-groupe du groupe unitaire.

Exercice 2.6.8 (i) Soient V une représentation irréductible de G et R sa représentation régulière. Soient $\lambda \in V^*$ une forme linéaire non nulle et H son noyau (donc un hyperplan de V). Vérifier la formule:

$$(\lambda \otimes e_1)^0(x) = \frac{1}{n} \sum_{g\in G} \lambda(g^{-1}x) e_g.$$

Montrer que cette application linéaire de V dans R est équivariante et que son noyau est $\bigcap_{g\in G} gH$. En déduire que, si V est irréductible, elle est isomorphe à une des composantes irréductibles de R.
(ii) Notant d_α le degré du type α et n_α sa multiplicité dans la décomposition de la représentation régulière, déduire des relations d'orthogonalité que $n_\alpha = d_\alpha$ puis que $\sum d_\alpha^2 = n$.

Exercice 2.6.9 Combien y a-t-il de caractères irréductibles sur $\mathfrak{S}_n$?

Part II

Corps

Chapter 1

Extensions de corps

1.0 Rappels et compléments

Dans tout ce chapitre et dans le suivant, les corps (et les anneaux) seront supposés commutatifs (seule exception: la preuve du théorème de Wedderburn à la section 2.4 du chapitre 2); et les anneaux seront supposés non triviaux ($0 \neq 1$).

1. Soient K un corps et soit $f : \mathbf{Z} \to K$ l'unique morphisme d'anneaux.

   - Si f est injectif, on dit que K est de caractéristique nulle. On identifie $\mathbf{Z}$ à son image. Le sous-corps engendré par $\mathbf{Z} \subset K$ est le plus petit sous-corps de K, il est isomorphe à $\mathbf{Q}$ (isomorphisme unique) et on les identifie.
   - Sinon, $\mathrm{Ker} f = p\mathbf{Z}$ où p est premier, on dit que K est de caractéristique p. L'image de f est le plus petit sous-corps de K, elle est isomorphe à $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ et on les identifie.

   Dans les deux cas, le plus petit-sous-corps de K est appelé *corps premier*.

2. Tout anneau intègre A se plonge de façon "essentiellement unique " dans un corps K qui est "minimal ": tout morphisme d'anneaux de A dans un corps L s'étend de manière unique en un morphisme $K \to L$. On a $K = \{a/b \mid a, b \in A\,;\ b \neq 0\}$; c'est le corps des factions de A.

3. Le corps des fractions de $\mathbf{Z}$ est $\mathbf{Q}$, celui de $K[X_1, \ldots, X_n]$ est $K(X_1, \ldots, X_n)$ (K étant un corps).

4. Soit I un idéal de l'anneau A. Alors A/I est un corps si, et seulement si, I est maximal.

5. Soient $P \in K[X]$ et $\alpha \in K$. Alors:

$$X - \alpha | P \Longleftrightarrow P(\alpha) = 0 \quad \text{et } (X-\alpha)^2 | P \Longleftrightarrow P(\alpha) = P'(\alpha) = 0.$$

   Noter que cette dernière équivalence est valable en toutes caractéristiques.

6. Soit $(X_i)_{i \in I}$ une famille infinie d'indéterminées. Il existe un unique anneau $K[(X_i)_{i\in I}]$ de polynômes en les X_i qui soit la réunion de tous les $K[(X_j)_{j\in J}]$, $J \subset I$ fini. Cet anneau est intègre et son corps des fractions $K((X_i)_{i\in I})$ est la réunion de tous les $K((X_j)_{j\in J})$, $J \subset I$ fini.

1.1 Notion d'extension

Lemme 1.1.1 *Soient K un corps et A un anneau. Alors tout morphisme de K dans A est injectif.*

Preuve. - Son noyau est un idéal de K ne contenant pas 1. □

On identifie alors K à son image et l'on dit que A est une K-algèbre. C'est à la fois un K-espace vectoriel et un anneau, et la multiplication est K-bilinéaire[1].

Définition 1.1.2 Si L est un corps et une K-algèbre, on dit que c'est une *extension* de K; notation: L/K. (Ne pas confondre avec un quotient !)

Le fait qu'alors L soit de manière canonique un K-espace vectoriel est extrêmement utile.

Exemples 1.1.3

1. $\mathbf{C}/\mathbf{R}$ et $\mathbf{R}/\mathbf{Q}$.
2. $K/\mathbf{Q}$ ou $K/\mathbf{F}_p$ (selon la caractéristique de K).
3. $K(X)/K$, $K(X,Y)/K$, $K(X,Y)/K(X)$.
4. Soit $P \in K[X]$ irréductible. Alors $L := K[X]/(P)$ est un corps et L/K est une extension. Notant $\alpha \in L$ la classe de X modulo l'idéal P, on a $L = K(\alpha)$ (sous-corps de L engendré par K et α), d'où la notation $K(\alpha)/K$.
5. Si M/L et L/K sont des extensions, M/K est une extension et L/K en est une *sous-extension* (on dit également *extension intermédiaire*).

Proposition 1.1.4 *Soit L/K une extension et soit $E \subset L$ un sous-ensemble.*
(i) L'intersection de toutes les sous-extensions contenant E est une sous-extension $K(E)/K$ dite engendrée par E.
(ii) Notant $(X_e)_{e\in E}$ une famille d'indéterminées indexée par E, il y a un unique morphisme d'extensions $K((X_e)_{e\in E}) \to L$ *(autrement dit, un morphisme de corps qui induit l'identité sur K) tel que $\forall e \in E$; $X_e \mapsto e$ et l'image de ce morphisme est $K(E)$.*

Preuve. - La preuve est mécanique et laissée au lecteur. □

Lorsque $E = \{x\}$, $x \in L$ (extension *monogène*), on note plutôt $K(x) := K(\{x\})$. De même, on note $K(x,y) := K(\{x,y\})$, etc.

Proposition 1.1.5 *Soient L/K et M/L deux extensions. Soient $(x_i)_{i\in I}$ une base du K-espace vectoriel L et $(y_j)_{j\in J}$ une base du L-espace vectoriel M. Alors $(x_i y_j)_{(i,j)\in I\times J}$ est une base du K-espace vectoriel M.*

Preuve. - Dans le calcul qui suit, le lecteur prendra garde à vérifier que toutes les combinaisons linéaires sont bien définies, autrement dit que les familles de coefficients sont à support fini.

- La famille $(x_i y_j)_{(i,j)\in I\times J}$ est génératrice: soit $z \in M$. Alors $z = \sum b_j y_j$ (les $b_j \in L$) et chaque $b_j \in L$ s'écrit $b_j = \sum a_{i,j} x_i$ (les $a_{i,j} \in K$), d'où $z = \sum a_{i,j} x_i y_j$.

[1] Tout cela peut s'étendre au cas d'un anneau non commutatif à condition de supposer que l'image de K dans A est centrale.

- La famille $(x_i y_j)_{(i,j)\in I\times J}$ est libre: supposons que $\sum a_{i,j}x_i y_j = 0$ (les $a_{i,j} \in K$) et notons pour tout j fixé $b_j := \sum a_{i,j}x_i \in L$. Alors $\sum b_j y_j = 0$, donc, pour tout j fixé, $b_j = \sum a_{i,j}x_i = 0$, d'où $a_{i,j} = 0$ pour tous i, j.

□

1.2 Éléments algébriques, éléments transcendants

Soit L/K une extension et soit $\alpha \in L$ (une bonne partie de ce qui suit est également valable pour une K-algèbre, le lecteur y réfléchira ...).

Premier cas: si les α^n, $n \in \mathbf{N}$, forment une famille libre sur K, on dit que α est *transcendant* sur K. Dans ce cas, le morphisme $K[X] \to L$, $P \mapsto P(\alpha)$ est injectif et son image $K[\alpha]$ (la sous-algèbre de L engendrée par α) est de dimension infinie. Ce n'est pas un corps, son corps des fractions est la sous-extension $K(\alpha)$ engendrée par α, qui est isomorphe au corps $K(X)$ des fractions rationnelles.

Exemples 1.2.1 Les nombres suivants sont transcendants sur $\mathbf{Q}$: $\sum_{n\geq 0} 10^{-n!}$ (Liouville); e (Hermite); π (Lindeman); "presque tous " les réels (Cantor).

Deuxième cas: si les α^n, $n \in \mathbf{N}$, forment une famille liée sur K, on dit que α est *algébrique* sur K. Le noyau du morphisme $K[X] \to L$, $P \mapsto P(\alpha)$ est engendré par un unique polynôme unitaire irréductible $\mu_{\alpha,K}$ appelé *polynôme minimal de* α. Son image $K[\alpha]$ est de dimension finie égale à $\deg \mu_{\alpha,K}$, c'est le *degré de* α *sur* K. De plus, $K[\alpha]$ est un corps, donc égal à $K(\alpha)$.

Exemples 1.2.2 Les nombres suivants sont algébriques sur $\mathbf{Q}$: i, $\sqrt{2}$, $e^{2k\mathrm{i}\pi/n}$, $\cos 2\pi/17$. Ils sont *ipso facto* algébriques sur $\mathbf{R}$ mais le degré n'est pas nécessairement le même: $\mu_{\mathrm{i},\mathbf{Q}} = \mu_{\mathrm{i},\mathbf{R}} = X^2 + 1$ (donc i est de degré 2 sur $\mathbf{R}$ comme sur $\mathbf{Q}$); mais $\mu_{\sqrt{2},\mathbf{Q}} = X^2 - 2$ (et $\sqrt{2}$ est donc de degré 2 sur $\mathbf{Q}$) alors que $\mu_{\sqrt{2},\mathbf{R}} = X - \sqrt{2}$ (et $\sqrt{2}$ est donc de degré 1 sur $\mathbf{R}$).

Exercice 1.2.3 Prouver que $\sqrt{2} + \sqrt{3}$ est algébrique sur $\mathbf{Q}$ et déterminer son polynôme minimal.

Remarque 1.2.4 Si α est algébrique sur K de caractéristique nulle, alors α est racine simple de $\mu_{\alpha,K}$: en effet, $\mu'_{\alpha,K}$ est alors de degré strictement plus petit. Cela reste vrai pour tout corps fini, et, plus généralement, pour tout corps de caractéristique $p > 0$ pour lequel l'application $x \mapsto x^p$ est surjective ("corps parfaits "), mais pas pour les autres corps. (Prendre par exemple $K := \mathbf{F}_p(X)$ et l'extension $K(X^{1/p}) := K[T]/(T^p - X)$: alors $\alpha := X^{1/p}$ est racine multiple de son polynôme minimal.)

1.3 Extensions finies

Définition 1.3.1 Une *extension finie* est une extension L/K telle que le K-espace vectoriel L est de dimension finie. Le *degré* de cette extension, noté $[L : K]$ (à ne pas confondre avec l'indice d'un sous-groupe !) est égal à cette dimension: $[L : K] := \dim_K L$.

Exercice 1.3.2 L'extension $\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q}$ a pour base $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$.

Exemple 1.3.3 Si α est algébrique sur K, on a $[K(\alpha):K] = \deg \mu_{\alpha,K}$. Sinon, $K(\alpha)$ n'est pas une extension finie.

Théorème 1.3.4 *Soient M/K et K/L deux extensions. Alors M/K est finie si, et seulement si, M/L et L/K le sont; et l'on a alors $[M:K] = [M:L][L:K]$.*

Preuve. - Si M/K est finie, L/K l'est aussi car L est sous-espace du K-espace de dimension finie M, donc est lui-même de dimension finie; et M/L l'est car tout système générateur fini du K-espace vectoriel M l'est *a fortiori* pour le L-espace M.
La réciproque et l'égalité découlent immédiatement de la proposition 1.1.5. □

Exercice 1.3.5 Comparer $\mathbf{Q}(\sqrt{2},\sqrt{3})$ à $\mathbf{Q}(\sqrt{2}+\sqrt{3})$.

Corollaire 1.3.6 *Soit L/K une extension finie. Alors tout élément de L est algébrique sur K.*

Remarque 1.3.7 La réciproque est fausse: par exemple la *clôture algébrique* $\overline{\mathbf{Q}}$ de $\mathbf{Q}$, qui est l'ensemble de tous les nombres complexes algébriques sur $\mathbf{Q}$, n'est pas une extension finie de $\mathbf{Q}$.

Signalons sans démonstration (*cf.* Lang) le théorème suivant:

Théorème 1.3.8 (Théorème de l'élément primitif) *Soit L/K une extension finie d'un corps K de caractéristique nulle, ou fini (ou plus généralement "parfait "). Il existe alors $\alpha \in L$ tel que $L = K(\alpha)$.*

□

1.4 Extensions quadratiques

Soit L/K une extension et soit $\alpha \in L \setminus K$ tel que $\alpha^2 = d \in K$. Alors $\mu_{\alpha,K} = X^2 - d$. On a:

$$K(\alpha) = K \oplus K\alpha = \{a + b\alpha \mid a,b \in K\}.$$

Les $\alpha' \in K(\alpha)$ tels que $K(\alpha') = K(\alpha)$ sont les $\alpha' = a + b\alpha$, $a,b \in K$, $b \neq 0$. Ce corps est noté $K(\sqrt{d})$. On a $K(\sqrt{d}) = K(\sqrt{d'})$ si, et seulement si, $d' = b^2 d$ où $b \in K^*$.

Exemples 1.4.1 On a $\mathbf{C} = \mathbf{R}(\sqrt{-1})$ et $\mathbf{Q}(\sqrt{-2}) = \mathbf{Q}(\mathrm{i}\sqrt{2})$. Le corps $\mathbf{Q}(\sqrt{-1}) = \mathbf{Q}(\mathrm{i})$ est le corps des fractions de l'anneau $\mathbf{Z}[\mathrm{i}]$ des entiers de Gauß.

Réciproquement, soit K'/K une extension de degré $[K':K] = 2$, ou *extension quadratique*. On suppose de plus que K n'est pas de caractéristique 2. Alors K' est de la forme $K(\sqrt{d})$. En effet, si $x \in K' \setminus K$, alors $x^2 \in K + Kx$, *i.e.* $x^2 = p + qx$, $p,q \in K$; et l'on peut prendre $d := (2x-q)^2 = q^2 + 4p$. En revanche, si K est de caractéristique 2, il peut y avoir des extensions quadratiques qui ne sont pas de cette forme.

Exercice 1.4.2 Tous les éléments de $\mathbf{F}_2$ sont des carrés et l'unique extension quadratique de $\mathbf{F}_2$ est $\mathbf{F}_2[X]/(X^2+X+1)$.

1.5 Extensions cyclotomiques

Encore des rappels et compléments

1. Le groupe μ_n des racines $n^{\text{èmes}}$ de l'unité dans $\mathbf{C}$ est un sous-groupe cyclique de $\mathbf{C}^*$. Ses générateurs (les *racines primitives $n^{èmes}$ de l'unité* dans $\mathbf{C}$) sont les $e^{2ki\pi/n}$, $k \in \{0,\dots,n-1\}$, $k \wedge n = 1$. Leur nombre est $\phi(n)$ (indicatrice d'Euler). Le nombre des éléments d'ordre $d|n$ dans μ_n est $\phi(d)$; on a donc $\sum_{d|n} \phi(d) = n$.

   Les μ_n sont les seuls sous-groupes finis de $\mathbf{C}^*$.

2. La fonction de Möbius $\mu : \mathbf{N}^* \to \{-1,0,1\} \subset \mathbf{N}$ est définie ainsi:

   - si n est divisible par un carré non trivial, $\mu(n) := 0$;
   - si n est quadratfrei, $n = p_1 \cdots p_k$ (des nombres premiers distincts), alors $\mu(n) := (-1)^k$; par exemple $\mu(1) = 1$.

   La fonction μ est multiplicative: si $a \wedge b = 1$, alors $\mu(ab) = \mu(a)\mu(b)$. Elle vérifie la *formule d'inversion de Möbius*: si $f, g : \mathbf{N}^* \to G$ sont à valeurs dans un groupe commutatif G, ici noté additivement[2] et si:

   $$\forall n \in \mathbf{N}^*\ ,\ g(n) = \sum_{d|n} f(d),$$

   alors:

   $$\forall n \in \mathbf{N}^*\ ,\ f(n) = \sum_{d|n} \mu(d) g(n/d) = \sum_{d|n} \mu(n/d) g(d).$$

   Par exemple, puisque $\sum_{d|n} \phi(d) = n$, on a $\phi(n) = \sum_{d|n} d\mu(n/d) = \sum_{d|n} (n/d)\mu(d)$.

3. Si $P, Q \in \mathbf{Q}[X]$ sont unitaires et tels que $PQ \in \mathbf{Z}[X]$, alors $P \in \mathbf{Z}[X]$ et $Q \in \mathbf{Z}[X]$ (la preuve utilise les décompositions $P = aP_1$, $Q = bQ_1$, où a et b sont les contenus de P et Q et où $P_1, Q_1 \in \mathbf{Z}[X]$ sont primitifs).

Proposition 1.5.1 *Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.*

Preuve. - Soient K un corps (commutatif) et $G \subset K^*$ un sous-groupe fini. Notons $n := |G|$. Pour tout d divisant n, notons $\psi(d)$ le nombre d'éléments de G d'ordre exact d: d'après le théorème de Lagrange, on a donc $\sum_{d|n} \psi(d) = n$.

Soit d un diviseur de n tel que $\psi(d) \neq 0$ et soit $x \in G$ un élément d'ordre d (il en existe puisque $\psi(d) \neq 0$). Le sous-groupe H engendré par x est cyclique d'ordre d et tous les $y \in H$ vérifient $y^d = 1$. Comme le polynôme $X^d - 1$ a au plus d racines (dans un corps commutatif quelconque), on a en fait: $y^d = 1 \Leftrightarrow y \in H$. En particulier, tous les éléments d'ordre exact d appartiennent à H; or, le nombre d'éléments d'ordre d dans un groupe cyclique d'ordre d est $\phi(d)$. On en déduit (toujours sous l'hypothèse que $\psi(d) \neq 0$) que $\psi(d) = \phi(d)$.

[2] Mais nous appliquerons également cette formule à des groupes notés multiplicativement.

On a donc les propriétés suivantes:

$$\begin{cases} \forall d|n\ ,\ \psi(d) \leq \phi(d), \\ \sum\limits_{d|n} \phi(d) = n, \\ \sum\limits_{d|n} \psi(d) = n. \end{cases}$$

On en déduit que $\forall d|n\ ,\ \psi(d) = \phi(d)$. En particulier, $\psi(n) = \phi(n) \neq 0$, donc G admet un élément d'ordre n, donc il est cyclique. □

Cyclotomie

Notons μ_n^* l'ensemble des racines primitives $n^{\text{èmes}}$ de l'unité dans $\mathbf{C}$. On a donc $|\mu_n^*| = \phi(n)$ et μ_n est la réunion disjointe des μ_d^* pour $d|n$.

Définition 1.5.2 Le $n^{\text{ème}}$ polynôme cyclotomique est:

$$\Phi_n(X) := \prod_{\zeta \in \mu_n^*} (X - \zeta) = \prod_{\substack{0 \leq k \leq n-1 \\ k \wedge n = 1}} \left(X - e^{2k\mathrm{i}\pi/n} \right).$$

C'est donc un polynôme unitaire de degré $\phi(n)$.

Proposition 1.5.3 *(i)* $\prod\limits_{d|n} \Phi_d(X) = X^n - 1$.
(ii) $\Phi_n(X) \in \mathbf{Z}[X]$.

Preuve. - (i) traduit le fait que $X^n - 1 = \prod\limits_{\zeta \in \mu_n} (X - \zeta)$ et que μ_n est la réunion disjointe des μ_d^* pour $d|n$.
(ii) Se prouve par récurrence forte sur n. On a bien entendu $\Phi_1 = X - 1$. Si les Φ_d, $d|n$, $d < n$, sont tous à coefficients entiers, leur produit P est unitaire et Φ_n est le quotient de $X^n - 1$ par P donc élément de $\mathbf{Z}[X]$. □

Corollaire 1.5.4

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)} = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}.$$

Preuve. - On applique la formule d'inversion de Möbius dans le groupe commutatif $\mathbf{Q}(X)^*$. □

Exemples 1.5.5

1. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = (X - j)(X - j^2) = X^2 + X + 1$, $\Phi_4(X) = (X - \mathrm{i})(X + \mathrm{i}) = X^2 + 1$, $\Phi_6(X) = (X + j)(X + j^2) = X^2 - X + 1$.
2. Si p est premier, $\Phi_p(X) = \dfrac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1$. On sait (critère d'Eisenstein, cours de L3) que ce polynôme est irréductible.

3. D'après le corollaire ci-dessus:

$$\Phi_6(X) = \frac{(X-1)(X^6-1)}{(X^2-1)(X^3-1)} = X^2 - X + 1.$$

$$\Phi_{12}(X) = \frac{(X^2-1)(X^{12}-1)}{(X^4-1)(X^6-1)} = X^4 - X^2 + 1.$$

Exercice 1.5.6 Soit $n = \prod p_i^{k_i}$ (décomposition en facteurs premiers, les $k_i \geq 1$). On note $n_0 := \prod p_i$ et $m := n/n_0$. Vérifier que $\Phi_n(X) = \Phi_{n_0}(X^m)$. Examiner le cas $n = 12$.

Théorème 1.5.7 (Gauß) *Le polynôme Φ_n est irréductible dans $\mathbf{Z}[X]$ et dans $\mathbf{Q}[X]$.*

Preuve. - Puisque $\Phi_n \in \mathbf{Z}[X]$ et qu'il est primitif (puisqu'unitaire), les deux assertions d'irréductibilité sont équivalentes.
Soit $\zeta \in \mu_n^*$ et soit $f := \mu_{\zeta,\mathbf{Q}}$ son polynôme minimal sur $\mathbf{Q}$, qui est irréductible et qui divise Φ_n. On va montrer que $f = \Phi_n$, ce qui suffira pour conclure. Pour cela, on va montrer que tous les éléments de μ_n^* sont racines de f.
Or tout tel élément est de la forme ζ^m avec $m \in \mathbf{N}^*$, $m \wedge n = 1$ (cela vient directement de l'isomorphie de μ_n avec $\mathbf{Z}/n\mathbf{Z}$ et du fait que les générateurs du groupe $\mathbf{Z}/n\mathbf{Z}$ sont les inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$). Il suffit donc de prouver que, si p est premier et ne divise pas n, alors ζ^p est racine de f: en effet, en itérant de telles puissances on obtiendra tous les ζ^m avec $m \in \mathbf{N}^*$, $m \wedge n = 1$, donc tous les éléments de μ_n^*. On est donc ramené au lemme ci-dessous. □

Lemme 1.5.8 *Avec les notations n, ζ, f, p ci-dessus, ζ^p est racine de f.*

Preuve. - On sait que ζ^p est racine de Φ_n. On va supposer qu'il n'est pas racine de f et aboutir à une contradiction.
On écrit $\Phi_n = fg$, où $f, g \in \mathbf{Z}[X]$ sont unitaires d'après les rappels. D'après l'hypothèse, ζ^p est racine de g, donc ζ est racine de $g(X^p)$. Son polynôme minimal f divise donc $g(X^p)$:

$$g(X^p) = f(X)h(X),$$

où $h \in \mathbf{Z}[X]$ est unitaire. On réduit modulo p cette relation, d'où une égalité dans $\mathbf{F}_p[X]$:

$$\overline{g}(X^p) = \overline{f}(X)\overline{h}(X).$$

Mais, dans $\mathbf{F}_p[X]$, l'application $x \mapsto x^p$ est un morphisme et c'est l'identité sur $\mathbf{F}_p$, de sorte que $\overline{g}(X^p) = \overline{g}(X)^p$:

$$\overline{g}^p = \overline{fh}.$$

Cela entraîne que les polynômes non constants $\overline{g}$ et $\overline{f}$ ont un facteur commun non constant et donc que le polynôme $\overline{\Phi_n} = \overline{f}\,\overline{g}$ a un facteur carré non constant, et donc qu'il en est de même de $X^n - \overline{1}$ (car c'en est un multiple). Or, si $Q^2|P$, on a $Q|P$ et $Q|P'$ (calcul immédiat). Avec $P = X^n - \overline{1}$ et $P' = \overline{n}X^{n-1}$, d'où ($\overline{n} \in \mathbf{F}_p$ étant, par hypothèse sur p, inversible) $\dfrac{X}{\overline{n}}P' - P = \overline{1}$, on voit que c'est bien impossible. □

Corollaire 1.5.9 *L'*extension cyclotomique $\mathbf{Q}(\zeta)$ *est la même quel que soit le choix de* $\zeta \in \mu_n^*$*; c'est une extension finie de degré* $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(n)$.

Remarque 1.5.10 L'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ est la plus petite contenant une racine de Φ_n ("corps de rupture " de Φ_n, *cf.* 1.7) et elle les contient en fait toutes ("corps de décomposition " de Φ_n, *cf.* 1.9).

1.6 Extensions algébriques

Définition 1.6.1 Une *extension algébrique* est une extension L/K telle que tout élément de L est algébrique sur K.

Proposition 1.6.2 *Toute extension finie est algébrique.*

Preuve. - En effet, si l'extension L/K est finie et si $\alpha \in L$, la dimension du sous-espace $K(\alpha)$ du K-espace vectoriel de dimension finie L est elle même finie (c'est le corollaire 1.3.6 page 29). □

Proposition 1.6.3 *Soit* L/K *une extension quelconque et soient* $\alpha, \beta \in L$ *des éléments algébriques sur* K*. Alors* $\alpha \pm \beta$ *et* $\alpha\beta$ *sont algébriques sur* K*, ainsi que* α^{-1} *si* $\alpha \neq 0$.

Preuve. - Il suffit, d'après la proposition précédente, de montrer que l'extension $K(\alpha,\beta)/K$ est finie; pour cela, il suffit de vérifier que les extentions $K(\alpha,\beta)/K(\alpha)$ et $K(\alpha)/K$ le sont. Or, α étant algébrique sur K, c'est vrai pour la seconde; et, β étant algébrique sur K, il l'est *a fortiori* sur $K(\alpha)$, donc c'est aussi vrai pour la première. □

Remarque 1.6.4 On donnera au chapitre 1 de la partie IV une méthode basée sur le résultant pour déterminer effectivement des polynômes annulateurs de $\alpha \pm \beta$ et $\alpha\beta$.

Exercice 1.6.5 Exprimer le polynôme minimal de α^{-1} en fonction de celui de α.

Corollaire 1.6.6 *L'extension* L/K *étant quelconque, l'ensemble des éléments de* L *algébriques sur* K *forme une sous-extension.*

Définition 1.6.7 Cette sous-extension est la *fermeture algébrique de* K *dans* L. Le corps K est dit *algébriquement fermé dans* L s'il est égal à sa fermeture algébrique dans L.

Proposition 1.6.8 *Soient* M/L *et* L/K *des extensions algébriques. Alors* M/K *est une extension algébrique.*

Preuve. - Soit $x \in M$ et soient $\alpha_1, \ldots, \alpha_n \in L$ tels que $x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n = 0$. L'extension $K(\alpha_1, \ldots, \alpha_n, x)/K(\alpha_1, \ldots, \alpha_n)$ est donc finie. Chaque extension $K(\alpha_1, \ldots, \alpha_{i+1})/K(\alpha_1, \ldots, \alpha_i)$ est fine car, α_{i+1} étant algébrique sur K, il l'est *a fortiori* sur $K(\alpha_1, \ldots, \alpha_i)$. L'extension composée $K(\alpha_1, \ldots, \alpha_n, x)/K$ est donc finie, d'où la conclusion. □

Corollaire 1.6.9 *L'extension* L/K *étant quelconque, la fermeture algébrique de* K *dans* L *est algébriquement fermée dans* L.

1.7 Corps de rupture

Définition 1.7.1 Soient K un corps et $P \in K[X]$ un polynôme irréductible. Une *extension de rupture* (on dit aussi *corps de rupture*) de P au dessus de K est une extension L/K dans laquelle P admet une racine α telle que $L = K(\alpha)$.

Proposition 1.7.2 *Toutes les extensions de rupture de P au dessus de K sont isomorphes à $K[X]/(P)$ (et donc isomorphes entre elles).*

Preuve. - Avec les notations de la définition, le morphisme de K-algèbres $F \mapsto F(\alpha)$ de $K[X]$ dans L est surjectif de noyau (P). □

Les exemples ci-dessous veulent illustrer le fait que l'unicité *à isomorphisme près* n'est pas exactement la même chose que l'unicité tout court.

Exemples 1.7.3

1. Soit d un entier quadratfrei différent de 0 et 1. Alors $\mathbf{Q}(\sqrt{d}) \subset \mathbf{C}$ est un corps de rupture de $X^2 - d$. C'est le seul qui soit inclus dans $\mathbf{C}$.
2. Soit $\zeta \in \mu_n^*$. Alors $\mathbf{Q}(\zeta)$ est un corps de rupture de Φ_n. C'est le seul qui soit inclus dans $\mathbf{C}$.
3. Chacun des corps $\mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{C}$, $\mathbf{Q}(j\sqrt[3]{2}) \subset \mathbf{C}$, $\mathbf{Q}(j^2\sqrt[3]{2}) \subset \mathbf{C}$, est un corps de rupture de $X^3 - 2$ au dessus de $\mathbf{Q}$. Ils sont deux à deux distincts.

La nuance est la suivante: si P est quadratique ou cyclotomique, toute extension qui contient une racine de P les contient toutes (et donc P est scindé dans cette extension); ce n'est pas vrai pour $P := X^3 - 2$. L'importance de cette nuance sera détaillée à la section 1.9.

1.8 Clôture algébrique

Rappelons qu'un corps K est dit *algébriquement clos* si tout polynôme non constant de $K[X]$ admet une racine dans K. On en déduit immédiatement que tout polynôme non constant de $K[X]$ est scindé dans K et que les irréductibles de $K[X]$ sont les polynômes de degré 1.

Proposition 1.8.1 *(i) Soit L/K une extension telle que L est algébriquement clos. Alors la fermeture algébrique K' de K dans L est un corps algébriquement clos.*
(ii) Toute extension algébrique L/K d'un corps algébriquement clos K est triviale, i.e. $L = K$.

Preuve. - Tout polynôme non constant de $K'[X]$ admet une racine dans L, et cette racine est dans K' car ce dernier est algébriquement fermé dans L d'après le corollaire de la proposition 1.6.8, ce qui prouve l'assertion (i). L'assertion (ii) en découle immédiatement. □

Définition 1.8.2 Une *clôture algébrique* du corps K est une extension algébrique L/K telle que L soit algébriquement clos.

Exemple 1.8.3 $\mathbf{C}$ est algébriquement clos.

Exercice 1.8.4 La fermeture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$ dans $\mathbf{C}$ est une clôture algébrique de $\mathbf{Q}$.

Proposition 1.8.5 *Soient L/K une extension algébrique et M/K une extension de K telle que M soit algébriquement clos. Il existe alors un* plongement *de L dans M, autrement dit, un morphisme d'extensions $\phi : L \to M$ (c'est-à-dire un morphisme de corps qui induit l'identité sur K).*

Preuve. - La preuve se fait en deux étapes. On suppose d'abord que $L = K(\alpha)$ pour un $\alpha \notin K$. Soit P le polynôme minimal de α sur K et soit $\beta \in M$ une racine de P. Il y a alors un unique ϕ tel que $\phi(\alpha) = \beta$.
Dans le cas général, on applique le lemme de Zorn à l'ensemble des couples (K', ϕ') tels que K'/K soit une sous-extension de L/K et ϕ' un morphisme d'extensions $K' \to M$, ordonné par la relation:

$$(K', \phi') \prec (K'', \phi'') \underset{def}{\iff} K' \subset K'' \text{ et } \phi''_{|K'} = \phi'.$$

Cet ensemble est inductif (arguments standards) et un élément maximal est nécessairement de la forme (L, ϕ) car sinon on pourrait lui appliquer la première étape. □

Théorème 1.8.6 (Steinitz) *Tout corps admet une clôture algébrique et celle-ci est unique à isomorphisme près.*

Preuve. - Avant de prouver l'existence, nous aurons besoin de trois petits lemmes.

Lemme 1.8.7 *Soient $P_1, \ldots, P_k \in K[X]$ non constants. Il existe une extension K'/K dans laquelle tous les P_i ont une racine.*

Preuve. - Il suffit de le prouver pour un polynôme puis d'itérer. Pour un polynôme, on prend une extension de rupture de l'un de ses facteurs irréductibles. □

Lemme 1.8.8 *Soit $(P_i)_{i \in I}$ une famille (pas nécessairement finie !) de polynômes non constants. Il existe une extension L/K dans laquelle tous les P_i ont une racine.*

Preuve. - Soient $\underline{X} := (X_i)$ une famille d'indéterminées indexée par I et $A := K[\underline{X}] := K[(X_i)]$. L'idéal $\mathfrak{A}$ engendré par les $P_i(X_i)$ est propre. En effet, s'il était égal à A, on aurait une relation:

$$\sum_{j \in J} Q_j(\underline{X}) P_j(X_j) = 1$$

pour un sous-ensemble fini $J \subset I$ et des $Q_j(\underline{X}) \in A$. D'après le lemme précédent, on pourrait choisir une extension L/K dans laquelle tous les P_j, $j \in J$ aient une racine α_j. En substituant X_j par α_j dans la relations ci-dessus (et X_i, $i \in I \setminus J$, par ce qu'on veut), on obtiendrait une contradiction.
Puisque $\mathfrak{A}$ est propre, il est inclus dans un idéal maximal $\mathfrak{M}$; on peut alors prendre $L := A/\mathfrak{M}$. □

Lemme 1.8.9 *Il existe une extension $\tilde{K}$ de K dans laquelle tous les polynômes non constants de $K[X]$ admettent une racine.*

Preuve. - On applique le lemme précédent à la famille de tous les polynômes non constants. □

Reprenons la démonstration du théorème.

Existence: Posons $K_0 := K$ et, pour tout n, $K_{n+1} := \tilde{K_n}$ (notation du lemme précédent). Alors $L := \bigcup_{n\in\mathbf{N}} K_n$ est une extension algébriquement close de K: en effet, tout polynôme non constant de $L[X]$ a tous ses coefficients dans l'un des K_n, donc une racine dans K_{n+1}. On peut alors prendre la fermeture algébrique de K dans L.

Exercice 1.8.10 Le corps L lui-même convient.

Unicité: Soient L/K et M/K deux clôtures algébriques. D'après la proposition qui précède le théorème, il existe un morphisme d'extensions de L dans M. Quitte à identifier, on a donc une extension composée $M/L/K$. Comme L est algébriquement clos et comme M/L est algébrique (car M/K l'est), on a $L = M$. □

1.9 Corps de décomposition, extensions normales

Dans cette section, qui arrive à la fin d'un long chapitre, aucune démonstration ne sera donnée. Cependant, les exemples qui suivent devraient permettre de "comprendre ce qui se passe ".

Soient K un corps, $\overline{K}$ une clôture algébrique de K et $f \in K[X]$ un polynôme irréductible. Notons $K(\alpha)$ le corps de rupture $K[X]/(f)$, où $\alpha := X \pmod P$. D'après la proposition 1.8.5, il existe un plongement de l'extension $K(\alpha)$ dans $\overline{K}$. En fait, notant $\alpha_1, \ldots, \alpha_m$ les racines de f dans $\overline{K}$, tout tel plongement est de la forme $P(\alpha) \mapsto P(\alpha_i)$ pour l'un des $i \in \{1, \ldots, m\}$ et le corps de rupture abstrait $K(\alpha)$ se "réalise " comme l'une des m extensions $K(\alpha_i)$. Ces extensions sont isomorphes à $K(\alpha)$, donc isomorphes entre elles, mais sont-elles distinctes ? Pour tenter de le comprendre on va supposer que $m = \deg f$, *i.e.* les α_i en sont des racines simples. (C'est certainement le cas si K est de caractéristique nulle ou fini ou plus généralement parfait.)

1. Si $f = aX^2 + bX + c$, $a, b, c \in K$, $a \neq 0$, on a $m = 2$, $\alpha_1 + \alpha_2 = -b/a$, donc $K(\alpha_1) = K(\alpha_2)$. En adjoignant à K une racine de f, on lui adjoint automatiquement l'autre.
2. Si $K = \mathbf{Q}$ et $f = \Phi_n$ (polynôme cyclotomique), on a $m = \phi(n)$ et si $\alpha_1 = e^{2ki\pi/n}$, $k \wedge n = 1$, tous les α_i sont des puissances de α_1 et les m corps $K(\alpha_i)$ sont encore égaux.
3. Si $K = \mathbf{Q}$ et $f = X^3 - 2$, les racines de f dans $\mathbf{C}$, donc dans la fermeture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$ dans $\mathbf{C}$ (qui est bien une clôture algébrique de $\mathbf{Q}$), sont $\alpha_1 := \sqrt[3]{2}$, $\alpha_2 := j\alpha_1$ et $\alpha_3 := j^2\alpha_1$ (où l'on note traditionnellement $j := e^{2i\pi/3}$). L'extension $K(\alpha_1)$ est incluse dans $\mathbf{R}$ et pas les deux autres, mais on peut vérifier directement que $K(\alpha_2) \neq K(\alpha_3)$.

Dans les deux premiers cas, l'extension de rupture contient toutes les racines de f, mais ce n'est pas vrai dans le dernier cas.

Définition 1.9.1 Soit $f \in K[X]$ un polynôme non constant. Une *extension de décomposition* (on dit aussi, et même plus fréquemment, *corps de décomposition*) de f est une extension L/K dans laquelle f est scindé et qui est engendrée (comme extension de K) par les racines de f:

$$\begin{cases} f(X) = c(X - \alpha_1)\cdots(X - \alpha_n), c \in K^*, \alpha_1, \ldots, \alpha_n \in L, \\ L = K(\alpha_1, \ldots, \alpha_n). \end{cases}$$

Proposition 1.9.2 *Les extensions de décomposition de f existent et sont isomorphes entre elles (en tant qu'extensions).*

□

La définition et la proposition ci-dessus se généralisent sans peine au cas d'une famille de polynômes. Il existe une caractérisation intrinsèque des extensions de décomposition. Pour en simplifier la formulation, nous fixons une clôture algébrique $\overline{K}$ de K et considérons seulement des sous-extensions de $\overline{K}$ (ce qui ne limite pas vraiment la généralité en vertu des résultats de la section 1.8). Notons que dans ce contexte, l'extension de décomposition d'une famille de polynômes est unique au sens propre: c'est la sous-extension de $\overline{K}$ engendrée par les racines de ces polynômes.

Théorème 1.9.3 *Soit L/K une sous-extension de $\overline{K}/K$. Les conditions suivantes sont équivalentes:*

1. *L est l'extension de décomposition d'une famille de polynômes.*
2. *Tout polynôme irréductible de $K[X]$ qui admet une racine dans L est scindé dans L.*
3. *Tout morphisme d'extension de L dans $\overline{K}$ envoie L dans L.*

□

Définition 1.9.4 Une telle extension est dite *normale* (ou "quasi-galoisienne " dans Bourbaki, mais cette terminologie est moins usitée).

Exemples 1.9.5
1. Toute extension quadratique de K est normale.
2. Toute extension cyclotomique de $\mathbf{Q}$ est normale.
3. L'extension $\mathbf{Q}\left(\sqrt[3]{2}\right)/\mathbf{Q}$ n'est pas normale.

Soit L/K une sous-extension normale de $\overline{K}/K$. D'après le troisième critère du théorème, les *plongements* de L dans $\overline{K}$ (c'est-à-dire les morphismes d'extension) sont en fait des automorphismes de L/K. Ils forment un groupe $\mathrm{Aut}(L/K)$.

Théorème 1.9.6 *(i) $|Aut(L/K)| \leq [L:K]$.*
*(ii) Il y a égalité si K est parfait (*i.e. *de caractéristique 0, ou de caractéristique $p>0$ et tel que $x \mapsto x^p$ soit un automorphisme de L: par exemple si K est fini).*

□

Lorsque $|\mathrm{Aut}(L/K)| = [L:K]$, l'extension L/K est dite *galoisienne* et $\mathrm{Aut}(L/K)$ est appelé *groupe de Galois* de l'extension et noté $\mathrm{Gal}(L/K)$.

Remarque 1.9.7 La clôture algébrique $\overline{K}$ étant fixée, toute extension normale L/K admet une unique image dans $\overline{K}$, *mais le plongement n'est pas unique*. Par exemple, il y a un unique corps de décomposition de X^2+1 dans $\overline{\mathbf{Q}}$, mais $\mathbf{Q}[X]/(X^2+1)$ s'y plonge de deux manières induites par $X \mapsto \pm \mathrm{i}$. Vues depuis l'extension de décomposition "intrinsèque" $\mathbf{Q}[X]/(X^2+1)$, les "réalisations" $+\mathrm{i}$ et $-\mathrm{i}$ sont indiscernables. Cette ambiguïté est au cœur de la théorie de Galois.

1.10 Exercices sur le chapitre "Extensions de corps "

Première série

Exercice 1.10.1 (i) Justifier toutes les affirmations non triviales de la section 1.4.
(ii) Décrire toutes les extensions quadratiques de $\mathbf{Q}$. (Elles sont paramétrées par les entiers quadratfrei autres que 0 et 1.)

Exercice 1.10.2 (i) Si $a \in \mathbf{Q}$, $a < 0$, on note $\sqrt{a} := \mathrm{i}\sqrt{-a}$. Soient $a, b \in \mathbf{Q}^*$ non carrés et tels que ab est non carré. Déterminer le polynôme minimal, le degré et les conjugués de $\sqrt{a}+\sqrt{b}$, puis le degré de la plus petite extension de $\mathbf{Q}$ contenant tous les conjugués.
(ii) Même question avec $\sqrt[3]{a}$ (pris dans son sens habituel).

Exercice 1.10.3 On dit que L/K est une *extension de type fini* s'il existe $E \subset L$ fini tel que $L = K(E)$. Si $E = \{x_1, \ldots, x_p\}$, on note $K(x_1, \ldots, x_p) := K(E)$. Démontrer l'équivalence logique:

$$L/K \text{ algébrique de type fini} \iff L/K \text{ finie.}$$

Exercice 1.10.4 Démontrer que $\overline{\mathbf{Q}}$ est dénombrable. Qu'en déduire concernant les nombres transcendants ? (Existence, probabilité ...)

Exercice 1.10.5 Soient K un corps et $K_0 \subset K$ son corps premier. Montrer que tout automorphisme de K induit l'identité sur K_0.

Deuxième série

Exercice 1.10.6 (i) Montrer que le seul[3] automorphisme du corps $\mathbf{R}$ est l'identité. (Indication: les nombres positifs et donc la relation d'ordre peuvent être caractérisés algébriquement.)
(ii) Montrer que les groupes $\mathbf{R}$ et $\mathbf{C}$ sont isomorphes[4]. (Indication: les considérer comme des espaces vectoriels sur $\mathbf{Q}$ et en mettre des bases en bijection.)

Exercice 1.10.7 (i) Calculer le groupe de Galois des extensions quadratiques et des extensions cyclotomiques de $\mathbf{Q}$.
(ii) Déterminer l'extension de décomposition du polynôme minimal de $\sqrt{2}+\sqrt{3}$ sur $\mathbf{Q}$ et son groupe de Galois.
(iii) Déterminer l'extension de décomposition du polynôme minimal de $\sqrt[3]{2}$ sur $\mathbf{Q}$ et son groupe de Galois.

Exercice 1.10.8 Justifier toutes les assertions non triviales de la section 1.9.

[3] On peut montrer qu'il y a une infinité non dénombrable d'automorphismes de $\mathbf{C}$.
[4] Cette bijection de la droite et du plan fit dire à Cantor, dans une lettre à Dedekind, "Je le vois mais ne le crois pas".

Chapter 2

Corps finis

2.1 Extensions quadratiques de $\mathbf{F}_p$

Soit p un nombre premier. Une extension quadratique de $\mathbf{F}_p$ est de la forme $\mathbf{F}_p[X]/(P)$, où $P = X^2 + aX + b$ est irréductible. Il y a p^2 polynômes unitaires de degré 2, ceux qui sont réductibles sont les $(X-\alpha)(X-\beta)$, au nombre de $p(p+1)/2$: il y a donc $p(p-1)/2$ polynômes unitaires irréductibles de degré 2.

Par exemple, pour $p = 2$, il y en a un seul, X^2+X+1. Le corps de rupture $\mathbf{F}_4 := \mathbf{F}_2[X]/(X^2+X+1)$ a quatre éléments, les $a+b\alpha$ où $a,b \in \{0,1\}$. La table d'addition correspondante est évidente (à isomorphisme près, c'est celle de $(\mathbf{Z}/2\mathbf{Z})^2$). La table de multiplication s'obtient en notant que $\alpha^2 = \alpha+1$, d'où $(a+b\alpha)(a'+b'\alpha) = (aa'+bb') + (ab'+ba'+bb')\alpha$:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

De même, il y a 3 polynômes unitaires irréductible de degré 2 sur $\mathbf{F}_3$, ce sont X^2+1, X^2+X-1 et X^2-X-1. Nous verrons que leurs corps de rupture sont isomorphes, mais on peut le vérifier directement en observant qu'ils s'obtiennent les uns à partir des autres par des substitutions $X \mapsto X \pm 1$. "Le" corps de rupture (bien déterminé à isomorphisme près) est isomorphe, en tant que groupe, à $(\mathbf{Z}/3\mathbf{Z})^2$, il est noté $\mathbf{F}_9$. On peut par exemple coder ses éléments $a+b\alpha$, $a,b \in \{0,\pm 1\}$ avec $\alpha^2 = -1$, d'où la même formule de multiplication que pour les nombres complexes: $(a+b\alpha)(a'+b'\alpha) = (aa'-bb') + (ab'+ba')\alpha$.

Si p est impair, l'endomorphisme $x \mapsto x^2$ du groupe $\mathbf{F}_p{}^*$ a pour noyau $\{\pm 1\}$, qui a deux éléments, son image a donc (d'après le premier théorème d'isomorphisme) $(p-1)/2$ éléments[1]; en comptant 0, il y a donc $(p+1)/2$ carrés dans $\mathbf{F}_p$, donc $(p-1)/2$ non carrés et donc $(p-1)/2$

[1] Ce sont les racines de $X^{(p-1)/2}-1$: en effet, tout carré x^2 vérifie $(x^2)^{(p-1)/2} = x^{p-1} = 1$ d'après le théorème de Lagrange, et le polynôme $X^{(p-1)/2}-1$ admet au plus $(p-1)/2$ racines.

polynômes irréductibles de la forme $X^2 - d$. Les substitutions $X \mapsto X + a$, $a \in \mathbf{F}_p$, en font $p(p-1)/2$ polynômes unitaires irréductibles de degré 2, en accord avec le dénombrement précédent.

2.2 Corps finis

Soit K un corps fini, commutatif d'après les hypothèses générales de cette partie[2]. On ne peut pas avoir $\mathbf{Q} \subset K$ car $\mathbf{Q}$ est infini. La caractéristique de K est donc un nombre premier p et le sous-corps premier est $\mathbf{F}_p$. L'extension $K/\mathbf{F}_p$ est finie car K lui-même est un système générateur fini du $\mathbf{F}_p$-espace vectoriel K. Soit $d := [K : \mathbf{F}_p]$ son degré. En tant qu'espace vectoriel, $K \simeq {\mathbf{F}_p}^d$. On a donc en particulier:

$$|K| = q := p^d.$$

Proposition 2.2.1 *Dans $K[X]$, on a la décomposition:*

$$X^q - X = \prod_{a \in K} (X - a).$$

Preuve. - Tout élément de K^* vérifie $a^{q-1} = 1$ d'après le théorème de Lagrange. Tout $a \in K$ est donc racine de $X^q - X$. Comme ce dernier est unitaire de degré q, la conclusion en découle. □

Proposition 2.2.2 *Le groupe K^* est cyclique.*

Preuve. - C'est un cas particulier de la proposition 1.5.1. □

Corollaire 2.2.3 *L'extension $K/\mathbf{F}_p$ admet un* élément primitif, i.e. *un $\alpha \in K$ tel que $K = \mathbf{F}_p(\alpha)$.*

Preuve. - N'importe quel générateur du groupe K^* convient. □

Notons qu'un tel élément primitif α a pour degré $[K : \mathbf{F}_p] = d$.

Proposition 2.2.4 *L'application $\theta_K : x \mapsto x^p$ est un automorphisme du corps K, l'*automorphisme de Frobenius. *Ses points fixes sont les éléments du corps premier $\mathbf{F}_p$. Le groupe $Aut(K/\mathbf{F}_p)$ des automorphismes de K est cyclique d'ordre d, engendré par θ_K.*

Preuve. - Il est évident que $(xy)^p = x^p y^p$. L'égalité $(x+y)^p = x^p + y^p$, valable en caractéristique p, vient de la formule du binôme et de ce que $p | \binom{p}{k}$ pour $1 \leq k \leq p-1$ (appliquer le lemme de Gauß à $k! | pN$, où $N = (p-1)\cdots(p-k+1)$). On a donc bien un endomorphisme d'anneau, nécessairement injectif puisque K est un corps (ou parce que son noyau ne contient que des nilpotents), donc bijectif puisque K est fini.
Tous les éléments de $\mathbf{F}_p$ sont racines de $X^p - X$, c'est-à-dire points fixes de θ_K; ce sont les seuls puisque ce polynôme est de degré p.
L'automorphisme θ_K^i est défini par $x \mapsto x^{p^i}$, ses points fixes sont racines de $X^{p^i} - X$, il y en a donc au plus p^i. Ainsi $\theta_K^i \neq \mathrm{Id}_K$ pour $i < d$. On a déjà vu que $\theta_K^d = \mathrm{Id}_K$ (c'est la relation $x^q = x$ pour tout $x \in K$).
Soit maintenant ϕ est un automorphisme quelconque de K. Il induit l'identité sur le corps premier

[2] Le théorème de Wedderburn, que l'on démontrera à la section 2.4, dit que tout corps fini est commutatif.

$\mathbf{F}_p$ (cela se déduit simplement du fait que $\phi(1) = 1$), ce qui explique la notation $\phi \in \mathrm{Aut}(K/\mathbf{F}_p)$. Soit α un élément primitif de $K/\mathbf{F}_p$; le degré de son polynôme minimal f sur $\mathbf{F}_p$ est donc d. Il a donc au plus d racines. De l'égalité $0 = \phi(f(\alpha)) = f(\phi(\alpha))$, on déduit que $\beta := \phi(\alpha)$ est l'une de ces racines. Or la donnée de β détermine complètement ϕ par la formule:

$$\phi\left(\sum_{i=0}^{d-1} a_i \alpha^i\right) = \sum_{i=0}^{d-1} a_i \beta^i.$$

Il y a donc au plus d éléments dans $\mathrm{Aut}(K/\mathbf{F}_p)$. Comme ce groupe contient le groupe cyclique d'ordre d engendré par θ_K, ils sont égaux. □

2.3 Sous-corps de $\overline{\mathbf{F}_p}$

On fixe un nombre premier p et une clôture algébrique $\overline{\mathbf{F}_p}$ de $\mathbf{F}_p$. On note $\theta : x \mapsto x^p$ l'*automorphisme de Frobenius* de $\overline{\mathbf{F}_p}$ (il est immédiat que c'en est bien un automorphisme).

Théorème 2.3.1 *Pour tout $d \geq 1$, notant $q := p^d$,*

$$\mathbf{F}_q := Fix(\theta^d) = \{x \in \overline{\mathbf{F}_p} \mid x^q = x\}$$

est l'unique sous-corps de $\overline{\mathbf{F}_p}$ ayant q éléments. Tout sous-corps fini de $\overline{\mathbf{F}_p}$ est l'un des $\mathbf{F}_q$. Notant $q' := p^{d'}$, on a $\mathbf{F}_q \subset \mathbf{F}_{q'}$ si, et seulement si, $d|d'$. Dans ce cas, $d' = de$, où $e := [\mathbf{F}_{q'} : \mathbf{F}_q]$.

Preuve. - Par définition, $Fix(\theta^d) = \{x \in \overline{\mathbf{F}_p} \mid x^q = x\}$. C'est le corps fixé d'un automorphisme, donc un sous-corps. Le polynôme $X^q - X$ a exactement q racines distinctes car il est de degré q sur un corps algébriquement clos et que son polynôme dérivé ne s'annule pas (c'est -1).
Tout corps fini à q éléments est inclus dans l'ensemble des racines de $X^q - X$ d'après la proposition 2.2.1.
Si $d' = de$, $\theta^{d'} = (\theta^d)^e$, d'où l'inclusion $Fix(\theta^d) \subset Fix(\theta^{d'})$. Réciproquement, si $\mathbf{F}_q \subset \mathbf{F}_{q'}$, l'extension est finie de degré e et $d' = de$. □

Théorème 2.3.2 *Tout corps fini de caractéristique p est isomorphe à un et un seul des $\mathbf{F}_q$.*

Preuve. - Cela découle de la proposition 1.8.5 et du téorème précédent. □

Théorème 2.3.3 *Le groupe $Aut(\mathbf{F}_{q'}/\mathbf{F}_q)$ des automorphismes de $\mathbf{F}_{q'}$ qui induisent l'identité sur $\mathbf{F}_q$ ("groupe de Galois de $\mathbf{F}_{q'}$ sur $\mathbf{F}_q$") est cyclique d'ordre $e = d'/d = [\mathbf{F}_{q'} : \mathbf{F}_q]$, engendré par θ^d.*

Preuve. - C'est un sous-groupe de $\mathrm{Aut}(\mathbf{F}_{q'}/\mathbf{F}_p)$, qui est cyclique engendré par la restriction de θ à $\mathbf{F}_{q'}$ d'après la proposition 2.2.4. Le reste est laissé au lecteur (exercice 2.5.8). □

2.4 Le théorème de Wedderburn

Théorème 2.4.1 (de Wedderburn) *Tout corps fini est commutatif.*

Preuve. - Soit K un corps fini *non supposé commutatif*. Le même argument que précédemment montre qu'il contient un corps premier $\mathbf{F}_p$; de plus, ce dernier est central. Le centre Z de K en est un sous-corps et c'est une extension de $\mathbf{F}_p$, donc $q := |Z|$ est de la forme p^d. Comme précédemment, K est un Z-espace vectoriel, donc $|K|$ est de la forme q^n. Notre but est de prouver que $n = 1$. Le groupe Z^*, qui est d'ordre $q-1$, est le centre du groupe K^*, qui est d'ordre $q^n - 1$. Le normalisateur de $x \in K^*$ dans K^* est le groupe des inversibles du corps $\{y \in K \mid yx = xy\}$, qui a q^{n_x} éléments pour un certain entier n_x. La formule des classes s'écrit donc ici:

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^{n_x} - 1}.$$

Exercice 2.4.2 Soient $a, b \in \mathbf{N}$; alors $q^a - 1 | q^b - 1 \Leftrightarrow a|b$.

Dans la formule ci-dessus, chaque n_x est donc un diviseur strict de n et donc chaque $\dfrac{q^n-1}{q^{n_x}-1}$ est divisible par $\Phi_n(q)$. On en déduit que $\Phi_n(q)$ divise $q-1$, mais on va voir que c'est impossible si $n > 1$, ce qui achèvera la preuve du théorème.
Si $n > 1$, pour tout $\zeta \in \mu_n^*$ on a $|\zeta| = 1$ et $\zeta \neq 1$, d'où, par l'inégalité triangulaire, $|q - \zeta| > q - 1$. On en déduit:

$$|\Phi_n(q)| = \prod_{\zeta \in \mu_n^*} |q - \zeta| > (q-1)^{\phi(n)} \geq q - 1,$$

ce qui contredirait le fait que $\Phi_n(q)$ divise $q-1$. □

2.5 Exercices sur le chapitre "Corps finis"

Première série

Exercice 2.5.1 Écrire les tables d'addition et de multiplication de $\mathbf{F}_8$ et $\mathbf{F}_9$.

Exercice 2.5.2 (i) Soit $a,n \in \mathbf{N}^*$. Si 2^n+1 est premier, alors n est une puissance de 2.
(ii) On note $F_k := 2^{2^k}+1$. (Si F_k est premier, c'est un *nombre premier de Fermat*.) Montrer suivant Euler que, si p premier divise F_k, alors $p \equiv 1 \pmod{2^k}$. (Raisonner sur l'ordre de $\overline{2}$ dans ${\mathbf{F}_p}^*$.)
(iii) F_4 et F_5 sont-ils premiers ? (Fermat le pensait.)
(iv) Regarder ce qui concerne les nombres premiers de Fermat dans Wikipedia.

Exercice 2.5.3 (i) Soient $a,n \in \mathbf{N}^*$. Si a^n-1 est premier, alors $a=2$ et n est premier.
(ii) Pour tout p premier, on note $M_p := 2^p-1$. (Si M_p est premier, c'est un *nombre premier de Mersenne*.) Montrer suivant Euler que, si q premier divise M_p, alors $q \equiv 1 \pmod{p}$. (Raisonner sur l'ordre de $\overline{2}$ dans ${\mathbf{F}_q}^*$.)
(iii) M_{11} et M_{13} sont-ils premiers ? Regarder ce qui concerne les nombres premiers de Mersenne dans Wikipedia (en particulier les records).

Exercice 2.5.4 Soit p un nombre premier impair.
(i) Montrer que $x \mapsto x^{(p-1)/2}$ est l'unique morphisme de ${\mathbf{F}_p}^*$ dans le groupe à deux éléments et déterminer son noyau.
(ii) En déduire une caractérisation des *résidus quadratiques modulo p* (*i.e.* les entiers n tels qu'il existe un entier a tel que $n \equiv a^2 \pmod{p}$).

Exercice 2.5.5 Soit L/K une extension du corps fini K et soit $\alpha \in L$ algébrique sur K. Montrer que α est racine simple de son polynôme minimal. (Ce résultat reste valable pour tout corps parfait.)

Exercice 2.5.6 (i) Soit K le corps de décomposition de X^8-1 sur $\mathbf{F}_p$. Montrer que $K = \mathbf{F}_p(x)$ où $x^4=-1$. Vérifier que $a := x+x^{-1}$ est tel que $a^2=2$. Montrer que 2 est un carré dans $\mathbf{F}_p$ si, et seulement si, $a^{p-1}=1$ et en déduire que dans tous les cas $a^p = \binom{2}{p}a$ (symbole de Legendre).
(ii) Des relations $a^p = x^p+x^{-p} = \begin{cases} a \text{ si } p \equiv \pm 1 \pmod 8, \\ -a \text{ si } p \equiv \pm 3 \pmod 8, \end{cases}$ déduire que $\binom{2}{p} = (-1)^{(p^2-1)/8}$.

Deuxième série

Exercice 2.5.7 (i) On note $I_{q,n}$ l'ensemble des polynômes irréductibles unitaires de degré n de $\mathbf{F}_q[X]$. Montrer que $X^{q^n}-X = \prod_{d|n} \prod_{P \in I_{q,d}} P$.
(ii) En déduire la formule $|I_{q,n}| = \dfrac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$.
(iii) Calculer $|I_{q,1}|$, $|I_{q,2}|$ et $|I_{q,3}|$ avec et sans cette formule.
(iv) Minorer $\sum_{d|n} \mu(d) q^{n/d}$ par $q^n - q^{n/2} - \cdots$ et en déduire que $I_{q,n} \neq 0$.

Exercice 2.5.8 (i) Achever la preuve du théorème 2.3.3.
(ii) Calculer $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$.
(iii) Décrire le groupe $\mathrm{Aut}(\overline{\mathbf{F}_p}/\mathbf{F}_p)$.