UVSQ 2005/2006
Master de sciences et technologie
MSMA110 (algèbre 1)

Algèbre 1, notes du cours

Distribuer au début le poly "structures abstraites".

Table des matières

1 Groupes et actions

1.1 Groupes

1.1.1 Définitions, premiers exemples

Lire le poly, définitions de groupe, sous-groupe, homomorphisme de groupes.

Premiers exemples de référence : $\mathbb{Z}$ et les $n\mathbb{Z}$ (les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, division euclidienne ; rappel ?) ; groupe symétrique fini, signature, groupe alterné (tester ce qu'ils savent) ; exponentielle et racines de l'unité ; groupe linéaire en dimension finie et sous-groupe des matrices triangulaires supérieures ; déterminant et groupe spécial linéaire.

Exercice : $f(H)$ et $f^{-1}(H')$ sont des sous-groupes. En particulier, définition du noyau ; c'est un sous-groupe.

Définition d'un produit direct de groupes à la naïve : produit de deux groupes puis d'un produit cartésien quelconque en donnant la loi (pas de considération catégorique ; plus tard ?). Associativité, commutativité à isomorphisme près.

Exemple de produits de $\mathbb{Z}/n\mathbb{Z}$; théorème chinois.

Exemple du groupe diédral D_{2n} (rotation $r : z \mapsto z \exp 2i\pi/n$ et symétrie axiale $s : z \mapsto \overline{z}$, $D_{2n} = \{r^j s^k,\ j, k\}$ sous-groupes C_n et $\mathbb{Z}/2\mathbb{Z}$). Ce n'est pas un produit direct de C_n et de $\mathbb{Z}/2\mathbb{Z}$ (centre).

Une intersection de sous-groupes est un sous-groupe. Définition du sous-groupe engendré par une partie comme intersection. Caractérisé comme un minimum pour l'inclusion (slogan intersection/plus-petit).

Exemples du diédral $D_{2n} = \langle r, s\rangle$, les transpositions engendrent le groupe symétrique, les transvections engendrent le groupe spécial linéaire (énoncé ; renvoi à Perrin), les symétries axiales engendrent les isométries planes (souvenir du Lycée ou cours de géométrie affine).

Définition de groupe monogène ou cyclique. Exercice : tout groupe monogène est isomorphe à $\mathbb{Z}$ ou à un $\mathbb{Z}/n\mathbb{Z}$.

1.1.2 Classes à gauche ou droite, quotients

Définition de sous-groupe distingué (ou normal). Les noyaux sont distingués (exo à la fin du chapitre : ce sont les seuls). Reprendre les exemples de 1.1.1. Exercice : H est distingué dans G ssi $xH = Hx$ pour tout x.

Définition de classes à droite (Hx) ou à gauche (xH) (deux relations d'équivalence ; savent-ils ce que c'est ?). Toutes ont le même cardinal (celui du sous-groupe H). Théorème de Lagrange $|G| = |H| \times [G : H]$ (preuve, partition de G). Le cardinal commun de $(G/H)_g$ et de $(G/H)_d$ est noté $[G : H]$: indice. Dans le cas fini, $|H|$ divise $|G|$.

Exercice : si $[G : H] = 2$, alors H est distingué dans G.

Envie de mettre sur $(G/H)_g$ la loi $xH.yH = xyH$. Pas de sens. Exemple détaillé des classes à droite et à gauche dans $\mathfrak{S}_3$ modulo le sous-groupe $\langle(12)\rangle$. MAIS, si (et

seulement si) H est distingué dans G, ça marche (preuve). Alors, $xH.yH = xyH$ définit une loi de groupe sur $(G/H)_g = (G/H)_d := G/H$ et la surjection canonique est un homomorphisme de groupes dont le noyau est H. Propriété universelle du quotient ($f : G \to G'$ se factorise si H normal et $H \subseteq \ker(f)$; conditions pour que l'homomorphisme induit soit injectif ou surjectif) ; premier théorème d'isomorphisme : $\boxed{G/\ker(f) \sim \mathrm{im}(f)}$.

Exemple : $GL/SL \sim k^*$; $\mathfrak{S}_n/\mathfrak{A}_n \sim \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \sim \mathbb{U}_n$ (racines n-ièmes de l'unité), $\mathbb{Q}/\mathbb{Z} \sim \mathbb{U}$ (racines de l'unité), $\mathbb{R}/\mathbb{Z} \sim S^1$ (cercle).

Deuxième théorème d'isomorphisme : $C \subseteq B$ distingués dans A. Alors B/C s'injecte canoniquement en un sous-groupe normal de A/C et $\boxed{(A/C)/(B/C) \sim A/B}$. [Preuve : factoriser $B \subseteq A \overset{can}{\to} A/C$ au travers de B/C pour l'injection canonique. Factoriser $A \overset{can}{\to} A/B$ en $A/C \to A/B$, puis ce dernier en $(A/C)/(B/C) \overset{f}{\to} A/B$. Par ailleurs, factoriser $A \overset{can}{\to} \overset{can}{\to} (A/C)/(B/C)$ en $A/B \overset{g}{\to} (A/C)/(B/C)$. Alors, f et g sont réciproques.]

Troisième théorème d'isomorphisme (exercice) : si A et B sont deux sous-groupes d'un même groupe G et si A normalise B (*i.e.* si $aBa^{-1} = B$ pour tout $a \in A$) alors $A \cap B$ est distingué dans A, $AB = \{ab, a \in A, \in B\} = BA$ est un sous-groupe de G, B est un sous-groupe distingué de AB et $\boxed{AB/B \sim A/A \cap B}$. [Preuve : $A \hookrightarrow AB \overset{can}{\to} AB/B$ a pour noyau $A \cap B$ et est surjectif.]

1.2 Action d'un groupe sur un ensemble

1.2.1 Définition, premiers exemples

Définition d'action (à gauche) de G sur X par homomorphisme de groupe $f : G \to \mathfrak{S}_X$ ou, de manière équivalente par application $G \times X \to X$ vérifiant $1.x = x$ et $g.(g'.x) = (gg').x$.

Variante : action à droite $(x.g).g' = x.(gg')$, c'est-à-dire une application $F : G \to \mathfrak{S}_X$ vérifiant $F(gg') = F(g')F(g)$. Quand on a une action à droite F, on obtient une action à gauche f en posant $f(g) = F(g^{-1})$.

Exemples : $\mathfrak{S}_E$ opère sur E (et $\mathfrak{S}_n$ sur $\{1, \ldots, n\}$) ; si V est un espace vectoriel, $\mathrm{GL}(V)$ opère sur V, sur les droites de V, sur les sous-ev de dimension donnée, sur les drapeaux ; $\mathrm{SL}_2(\mathbb{R})$ opère sur le demi-plan de poincaré *via* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \frac{az+b}{cz+d}$ (exo) ; les similitudes du plan agissent sur l'ensemble des cercles ; les isométries du plan fixant l'origine agissent sur le cercle trigonométrique ; les isométries du plan qui stabilisent un polygone régulier donné agissent sur ses sommets, sur les milieux de ses arêtes ; les isométries de l'espace qui stabilisent un cube agissent sur ses diagonales. Un groupe agit sur lui-même par conjugaison ou par translation à gauche.

Définition d'action transitive ($\forall x, y, \exists g, y = g.x$) ou fidèle (seul 1 fixe tous les points). Si f est une action de G, elle se factorise en une action fidèle de $G/\ker(f)$.

Définition d'orbite d'un point (notée $G.x$), de sous-groupe d'isotropie (noté G_x). Les sous-groupes d'isotropie des points d'une même orbite sont conjugués ($G_{g.x} = gG_xg^{-1}$). Relation d'équivalence $x \sim y \Leftrightarrow \exists g, y = g.x$. Les classes sont les orbites. Elles forment une partition de X.

Une partie Y de X est dite stable lorsque $G.Y \subseteq Y$ (en fait, égalité *via* les g^{-1}). Définition de stabilisateur d'une partie (sous-groupe des éléments du groupe qui stabilisent la partie).

Définition de partie fixe ($\forall y, g,\ g.y = y$) et de fixateur d'une partie (éléments du groupe qui fixent la partie).

Exemple : $u \in \mathrm{GL}(V)$, action naturelle de $\langle u \rangle$ sur V. Une droite stable est une droite de vecteurs propres pour u. Une droite fixe est une droite propre associée à la valeur propre 1.

Si H est un sous-groupe de G, action par conjugaison de G sur lui-même. Stabilisateur de H s'appelle normalisateur ; fixateur de H s'appelle centralisateur. Centre d'un groupe.

1.2.2 Equation aux classes

Si x est dans X, l'application $g \mapsto g.x$ est constante sur les classes à gauche modulo G_x. Elle induit une bijection de l'ensemble $(G/G_x)_g$ sur l'orbite $G.x$. Ainsi, $\mathrm{Card}(G.x) = [G : G_x]$.

Dans le cas où X est un ensemble fini, l'équation aux classes traduit la partition de X en orbites sous l'action de G en termes de cardinaux : $\mathrm{Card}(X) = \sum_{x \in \mathcal{R}} [G : G_x]$ ou $\mathcal{R}$ est un système de représentants des classes à gauche (ou à droite).

Exemple des p-groupes : si X^G désigne les invariants sous G et si G est un p-groupe, alors $\mathrm{Card}(X) \equiv \mathrm{Card}(X^G)\ [p]$. Exemple de l'action de G sur lui-même par conjugaison : le centre d'un p-groupe est non trivial (et exo : un p-groupe est nilpotent (donc résoluble), récurrence sur l'exposant de l'ordre).

Exemple : action du groupe positif du cube sur les centres des faces. Transitive, 6 centres, isotropie d'ordre 4 : le groupe positif du cube est d'ordre 24.

1.2.3 Produit semi-direct

Suite exacte de groupes, suite exacte scindée (existence d'une section ou existence d'un sous-groupe qui fait de la surjection un isomorphisme par restriction).

Une suite exacte $1 \to N \to G \to Q \to 1$ est scindée si, et seulement s'il existe un sous-groupe H de G tel que $H \cap N = 1$ et $G = HN$.

Définition du produit semi-direct de N et Q relatif à une action de Q sur N par automorphismes, *i.e.* un homomorphisme de groupes $\varphi : Q \to \mathrm{Aut}(N)$ (c'est la loi de groupes sur le produit cartésien définie par $(n, q)(n', q') = (n\varphi(q)(n'), qq')$, le neutre est $(1, 1)$, l'inverse de (n, q) est $(\varphi(q^{-1})(n^{-1}), q^{-1})$).

G est isomorphe à un produit semi-direct de Q et N si, et seulement s'il existe une suite exacte scindée $1 \to N \to G \to Q \to 1$. En passant, formule du produit direct

interne $nhn'h' = nhn'h^{-1}hh'$.

Caractérisation du produit direct parmi les semi-directs (N et H commutent).

Exemples dans $\mathfrak{S}_n$, groupe diédral, groupe linéaire, groupe affine, isométries (dont celles des polyèdres réguliers ; groupe du cube, groupe du tétraèdre).

1.3 Groupes abéliens finis

Théorème : *si G est un groupe abélien fini, il est isomorphe à un produit de groupes cycliques $G \sim \mathbb{Z}/n_1\mathbb{Z} \times \dots \mathbb{Z}/n_r\mathbb{Z}$. Il n'y a pas unicité en général. Il y a unicité si on exige $n_1|n_2|\dots|n_r$.*

Preuve. 1- On suppose d'abord que G est un p-groupe abélien d'ordre p^m. Existence : on procède par récurrence sur m. Soit a_1 un élément de G d'ordre maximal et $G_1 = \langle a_1 \rangle$. On dévisse G/G_1 par hypothèse de récurrence. On relève ses sous-groupes cycliques (on peut). Unicité : récurrence encore. On l'applique au sous-groupe pG. 2- Pour tout nombre premier p, on définit le sous-groupe de p-torsion de G par $G(p) = \{g \in G,\ \exists m \in \mathbb{N},\ p^m g = 0\}$, sous-groupe des éléments dont l'ordre est une puissance de p (remarquer que si $|G| = \prod_{1 \leq k \leq s} p_k^{a_k}$, on peut ajouter $m \leq a_k$ dans la définition de la p-torsion, Bézout). On montre que $G = \oplus_{1 \leq k \leq s} G(p_k)$ par récurrence sur s (Bézout). Pour l'existence d'une décomposition avec les conditions de divisibilité des n_k, regrouper les facteurs à la chinoise par puissances maximales. Unicité : se convaincre qu'il n'y a qu'une seule manière de regrouper les facteurs à la chinoise. On aura une preuve formalisée plus tard.
[NB : Bézout intervient beaucoup. On y reviendra.]

Les nombres n_k qui se divisent sont appelés facteurs invariants du gaf.

Exercice : a et b des entiers ; quels sont les facteurs invariants de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$? Et trois facteurs ?

1.4 Présentations d'un groupe, groupes libres

1.4.1 Groupe libre

[Introduction sur la définition d'une application linéaire par image arbitraire d'une base. Faire pareil dans le cadre des groupes ?]

Si L est un groupe et X une partie de L, on dit que L est *libre* sur X lorsque toute application $X \to G$ dans n'importe quel groupe G se prolonge en un homomorphisme de groupes $L \to G$ (diagramme commutatif à dessiner ; définition par propriété universelle ; petit speech léger sur les catégories).

Théorème *Pour tout ensemble X, il existe un groupe libre sur X, unique à isomorphisme près.*

Preuve de l'unicité. Preuve de l'existence au paragraphe suivant (on le construit). Idée : construire des mots dans l'alphabet $X \cup X^{-1}$, réduire quand on peut.

Si L est libre sur X et sur Y, alors X et Y ont le même cardinal. Ce cardinal est le *rang* du groupe libre. Preuve (dans le cas fini) : si $\mathrm{Card}(X) = n$, toute application

$X \to \mathbb{Z}/2\mathbb{Z}$ se prolonge en un homomorphisme de groupes $L \to \mathbb{Z}/2\mathbb{Z}$; ainsi, le cardinal de l'ensemble des homomorphismes de groupes de L sur $Z/2\mathbb{Z}$ est-il 2^n : L détermine n.

Exercice : si L est un groupe libre sur un ensemble X, alors $L/[L,L]$ est isomorphe à $\mathbb{Z}^{(X)}$ (*groupe abélien libre*).

1.4.2 Produit libre de groupes

Si $(G_i)_{i\in I}$ est une famille de groupes, soit A leur union disjointe (définir, c'est la partie de $(\cup_i G_i) \times I$ formée des (g,i) tels que $g \in G_i$). Soit $M(A)$ l'ensemble des mots de A (*i.e.* l'ensemble des suites finies déléments de A), que l'on munit de la concaténation (loi interne, associative, le mot vide est neutre ; ça en fait un *monoïde*). On définit sur $M(A)$ la relation d'équivalence engendrée (définir) par les relations $me_im' \sim mm'$ si e_i est le neutre de G_i et $mgg'm' \sim mg''m'$ si g, g', g'' sont dans un même G_i et vérifient $gg' = g''$. Cette relation d'équivalence est compatible avec la concaténation et l'ensemble quotient $M(A)/\sim$ est un groupe pour la loi induite. C'est, par définition, le *produit libre* des G_i. On le note $*_{i\in I}G_i$.

Par exemple, dans un produit libre, l'inverse de la classe d'un mot $a_1 \dots a_n$ est la classe de $a_n^{-1} \dots a_1^{-1}$.

Définition de mot réduit. Tout mot de l'union disjointe est équivalent à un unique mot réduit. Conséquence : les homomorphismes canoniques $G_i \to *_{i\in I}G_i$ (où l'image de g_i est la classe du mot g_i de longueur 1) sont injectifs.

Propriété universelle du produit libre : si $f_i : G_i \to G$ est une famille d'homomorphismes dans un même groupe G, il existe un unique homomorphisme de groupes $f : *_{i\in I}G_i \to G$ qui factorise tous les f_i par les injections canoniques.

Si X est un ensemble, le produit libre $*_{x\in X}\mathbb{Z}$ est un groupe libre ; et voilà pour son existence.

[Renvoyer *Topics in geometric group theory* de P. de la Harpe.]

Notion importante en topologie (groupe fondamental).

Théorème de Nielsen-Schreier *Tout sous-groupe d'un groupe libre est libre.* On l'admet. Il existe des preuves topologiques simples, à condition d'avoir le groupe fondamental à sa disposition. Attention, le rang d'un sous-groupe peut être plus grand. On peut montrer que si L est libre et H est un sous-groupe de L, alors $\mathrm{rg}(H) = [L : H](\mathrm{rg}(L) - 1) + 1$.

Noter que le groupe libre sur un singleton est $\mathbb{Z}$, quand même.

1.4.3 Présentations d'un groupe

Tout groupe est isomorphe au quotient d'un groupe libre (le groupe libre sur le groupe, par exemple, ou sur un système de générateurs).

Si X est un système de générateurs de G et si R est le noyau (libre, sous-groupe des relations) de $L(X) \to G$ de telle sorte que $G \sim L(X)/R$, la donnée de X et de R est appelée une présentation de G. On note $G \sim \langle X, R\rangle$.

Exemple de $\mathbb{Z}/n\mathbb{Z} = \langle x; x^n \rangle$. Exemple du groupe diédral $D_{2n} \sim \langle x, y; x^n = y^2 = 1, (xy)^2 = 1 \rangle$ (le groupe présenté, ensemble des $x^k y^l$ a un cardinal $\leq 2n$, et surjection de ce groupe dans D_{2n}). Attention, ici, x^n, y^2, $(xy)^2$ ne forme pas une base de R : R est la clôture normale du sous-groupe engendré par x^n, y^2 et $(xy)^2$.

Il n'y pas unicité des présentations (mais pas du tout).

Petit mot sur le problème de Burnside : si G est un groupe ayant un nombre fini de générateur et si les éléments de G sont tous d'ordres $\leq n$ pour un n donné, G est-il fini ? Résultat récent : en général, le groupe $L/\langle x^n, x \in L \rangle$ n'est pas fini.

1.5 Réseaux

Un sous-groupe de $\mathbb{R}^n$ est discret lorsque son intersection avec tout compact est fini (définition ; exo : pareil que de dire qu'il est fermé et que la topologie induite par l'usuelle sur le sous-groupe est la discrète). Par exemple $\mathbb{Z}^n$.

Théorème *Un sous-groupe Γ de $\mathbb{R}^n$ est discret si, et seulement s'il existe un entier naturel $r \leq n$ et des vecteurs $v_1, \ldots, v_r$ linéairement indépendants sur $\mathbb{R}$ tels que $\Gamma = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_r$.*

Preuve par récurrence sur n. Prendre une famille $\mathbb{R}$-libre maximale $w_1, \ldots, w_r$ de Γ et K le polytope compact sur les w_k. Tout élément de Γ se décompose sur les w_k (caractère maximal) et ses coordonnées sont rationnelles (si $x = \sum x_k w_k \in \Gamma$, considérer les $x^{(m)} = mx - \sum_k \lfloor mx_k \rfloor w_k$ qui sont dans $\Gamma \cap K$: deux d'entre eux coïncident) ; en outre, le groupe Γ est engendré par $\Gamma \cap K$ (voir $x^{(1)}$). Soit d tel que $d\Gamma \subseteq \oplus_k \mathbb{Z}w_k$ et soit $x = \sum_{1 \leq k \leq r} x_k w_k$ dans Γ tel que dx_r soit un entier > 0 minimal parmi les r-ièmes coordonnées > 0 des éléments de $d\Gamma$. Alors, $\Gamma = \mathbb{Z}x \oplus \Gamma \cap V$ où $V = \oplus_{1 \leq k \leq r-1} \mathbb{R}w_k$ (division euclidienne par dx_r de $d\times$ la dernière coordonnée d'un élément de Γ ; reste est nul ; soustraire les vecteurs). On applique la récurrence au sous-groupe discret $\Gamma \cap V$ de V.

Lemme : si les groupes additifs $\mathbb{Z}^n$ et $\mathbb{Z}^m$ sont isomorphes, alors $n = m$. Preuve : si p est un nombre premier, un tel isomorphisme induit un isomorphisme de $\mathbb{F}_p$-espaces vectoriels entre $\mathbb{F}_p^n$ et $\mathbb{F}_p^m$. Le nombre r du théorème est unique ; on l'appelle rang de Γ. Un réseau est par définition un sous-groupe discret de rang maximal.

Exemple (Samuel page 66). Si $x \in \mathbb{R}^n$ a au moins une coordonnée irrationnelle, le sous-groupe additif H engendré par $\mathbb{Z}^n$ et x n'est pas discret (preuve du théorème : x serait combinaison linéaire rationnelle de la base canonique, donc rationnel). On peut approcher 0 arbitrairement près par des éléments non nuls de H : pour tout $\varepsilon > 0$, il existe des entiers q et p_k tels que $|x_k - p_k/q| \leq \varepsilon/q$ (speech sur l'approximation des réels par des rationnels).

Le volume (Lebesgue) du polytope des vecteurs d'une $\mathbb{Z}$-base d'un réseau ne dépend pas du choix de la $\mathbb{Z}$-base (déterminant ± 1 quand on change de $\mathbb{Z}$-base). On l'appelle volume du réseau.

Théorème de Minkowski *Γ un réseau de $\mathbb{R}^n$ et S une partie mesurable (Lebesgue) de $\mathbb{R}^n$ telle que $\mathrm{vol}(S) \geq \mathrm{vol}(\Gamma)$. Alors, il existe x et y dans S tels que $x - y \in \Gamma$.*

Corollaire : Γ un réseau de $\mathbb{R}^n$ et S une partie mesurable (Lebesgue) de $\mathbb{R}^n$, symétrique par rapport à 0 et convexe. On suppose que $\mathrm{vol}(S) > 2^n \mathrm{vol}(\Gamma)$. Alors $S \cap \Gamma$ n'est pas réduit à $\{0\}$ (idem avec $\mathrm{vol}(S) \geq 2^n \mathrm{vol}(\Gamma)$ si S est en outre compacte).

1.6 Théorèmes de Sylow

Définition d'un p-Sylow (p sous-groupe dont l'indice n'est pas divisible par p).

Exemple : les matrices trigonales sup avec des 1 sur la diagonale forment un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.

Premier théorème de Sylow *Tout groupe fini contient un p-Sylow.*

Preuve : voir G comme un sous-groupe de $\mathfrak{S}_n$ où n est l'ordre de G, puis comme un sous-groupe de $\mathrm{GL}(n, \mathbb{F}_p)$. Comme on a un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$, on conclut avec le lemme suivant.

Lemme *Soient G un groupe fini, H un sous-groupe, S un p-Sylow de G. Il existe $a \in G$ tel que $H \cap (aSa^{-1})$ soit un p-Sylow de H.*

Preuve. On fait agir H sur $(G/S)_g$ par translation à gauche et on écrit l'équation aux classes $[G : S] = \sum_{a \in \mathcal{R}} [H : H_{aS}]$. Comme p ne divise pas $[G : S]$, soit a tel que p ne divise pas $[H : H_{aS}]$: un tel a convient car $H_{aS} = H \cap (aSa^{-1})$ est un p-Sylow de H (c'est un p-groupe car c'est un sous-groupe du p-Sylow aSa^{-1}).

Deuxième théorème de Sylow *Tout p-sous-groupe est contenu dans un p-Sylow ; les p-Sylow sont conjugués.*

Preuve : avec le lemme, deux fois.

Remarque : un p-Sylow est distingué ss'il est le seul p-Sylow.

Troisième théorème de Sylow *Le nombre de p-Sylow divise l'ordre du groupe et est $\equiv 1$ $[p]$.*

Preuve. 1- Faire agir G par conjugaison sur l'ensemble $\mathcal{S}$ de ses p-Sylow. Une seule orbite. 2- Faire agir un p-Sylow S par conjugaison sur $\mathcal{S}$. Comme $\mathcal{S}$ est un p-groupe, $\#\mathcal{S} \equiv \#\mathcal{S}^S$ $[p]$. On montre que $\mathcal{S}^S = \{S\}$: si $T \in \mathcal{S}^S$, soit $N = \mathrm{Stab}_G(T)$; alors $T \lhd N$, donc T est l'unique p-Sylow de N. D'où $S = T$ puisque S est aussi un p-Sylow de N.

Exemples : un groupe d'ordre 91 n'est jamais simple (voir les 7-Sylow). Les 3-Sylow et les 2-Sylow de $\mathfrak{S}_4$.

Exercice : compter et décrire les Sylow de $\mathfrak{S}_3$, $\mathfrak{A}_4$, $\mathfrak{A}_5$, $\mathfrak{S}_5$.

1.7 Le groupe symétrique fini

Permutations d'un ensemble fini. Si deux ensembles sont equipotents, leurs groupes symétriques sont isomorphes. On note $\mathfrak{S}_n = \mathfrak{S}_{\{1,\ldots,n\}}$.

Exercice : $\mathrm{Card}(\mathfrak{S}_n) = n!$.

Définition d'un p-cycle de $\mathfrak{S}_n$, notation $(a_1, \ldots a_p)$, définition du support d'une permutation ; support d'un p-cycle.

Exercice : si $c = (a_0, \ldots, a_{p-1})$ et $m \in \mathbb{Z}$, alors $c^m(a_k) = a_{\overline{k+m}}$ où $\overline{k+m}$ est le reste de la division euclidienne de $k + m$ par p. L'ordre d'un p-cycle est p.

Remarque : $\mathfrak{S}_2 \sim \mathbb{Z}/2\mathbb{Z}$; si $n \geq 3$, $\mathfrak{S}_3$ n'est pas abélien ($(12)(23) \neq (23)(12)$).

Formule de conjugaison des cycles : $s(a_1, \ldots, a_p)s^{-1} = (s(a_1), \ldots, s(a_p))$. Tous les p-cycles sont conjugués dans $\mathfrak{S}_n$.

Deux cycles à supports disjoints commutent. Toute permutation se décompose en produit de cycles à supports disjoints, unicité à l'ordre près des facteurs.

Les transpositions engendrent $\mathfrak{S}_n$. Raffinement : les $(k, k+1)$ engendrent $\mathfrak{S}_n$.

Tout groupe fini est isomorphe à un sous-groupe d'un $\mathfrak{S}_n$. [Et tout groupe est isomorphe à un sous-groupe d'un $\mathfrak{S}_E$.]

Théorème *Si $n \geq 2$, il existe un unique homomorphisme de groupes $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ non trivial. Si c est un p-cycle, $\varepsilon(c) = (-1)^{p-1}$.*

On appelle ε la signature. Preuve de l'unicité par engendrement des transpositions ; preuve de l'existence par nombre d'inversions. Si s a m orbites, alors $\varepsilon(s) = (-1)^{n-m}$ (en effet, la somme des longueurs des orbites égale n).

Groupe alterné. C'est un sous-groupe distingué d'indice 2, engendré par les 3-cycles. Si $n \geq 5$, alors les 3-cycles sont tous conjugués dans $\mathfrak{A}_n$.

Cas du groupe de Klein $K = \langle (12)(34), (13)(24) \rangle$ dans $\mathfrak{A}_4$. Chaîne de sous-groupes distingués $\{1\} \triangleleft K \triangleleft \mathfrak{A}_4 \triangleleft \mathfrak{S}_4$. Cette situation est exceptionnelle.

Simplicité de $\mathfrak{A}_n$ lorsque $n \neq 4$ (preuve avec Sylow ou non).

Exercice : groupes dérivés (à définir) $D(\mathfrak{A}_n) = D(\mathfrak{S}_n) = \mathfrak{A}_n$ si $n \geq 5$. Calculer $D(\mathfrak{A}_4)$, $D(\mathfrak{A}_3)$, $D(\mathfrak{S}_4)$ et $D(\mathfrak{S}_3)$.

Si $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.

Exercice : si $n \geq 3$, le centre (à définir) de $\mathfrak{S}_n$ est trivial.

Exo possible (voir Perrin) : les automorphismes de $\mathfrak{S}_n$ sont intérieurs si $n \neq 6$.

2 Algèbre linéaire sur un corps

2.1 Suite exacte d'espaces vectoriels

Définition : une suite $\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \ldots$ d'applications linéaires entre k-espaces vectoriels est *exacte en* B lorsque $\mathrm{im}(f) = \ker(g)$. Une suite exacte courte est une suite $0 \to E' \xrightarrow{i} E \xrightarrow{s} E'' \to 0$ exacte en E', E et E'', *i.e.* i est injective, $\mathrm{im}(i) = \ker(s)$ et s est surjective (plus généralement, une suite est exacte lorsqu'elle est exacte partout).

Exemple (prototype) : si E' est un sous-ev de E, l'inclusion et la surjection canonique forment une suite exacte $0 \to E' \to E \to E/E' \to 0$ (définir le quotient s'il faut).

Dimensions et suites exactes ; deux ev sont isomorphes ss'ils ont même dimension.

Existence de bases d'un ev (Zorn), dimension, théorème de la base incomplète sous la forme d'existence de supplémentaires. Toute suite exacte d'ev est scindée.

2.2 Dualité dans les espaces vectoriels

Définition du dual, notation $\langle x, f\rangle$, forme bilinéaire canonique sur $E \times E^*$, fomres coordonnées, injection $\delta : V \to V^{**}$. Transposée d'une application linéaire.

En dimension finie, base duale, V et V^* sont isomorphes (non canoniquement), formes coordonnées, δ est un isomorphisme (canonique, lui). La matrice de la transposée est la transposée de la matrice dans la base duale. Diagramme commutatif entre f et ${}^{tt}f$.

En dimension quelconque, le dual de $k^{(I)}$ est k^I ; le cardinal décroche.

Suite exacte et passage au dual (encore exact), preuve de la surjectivité (existence d'un supplémentaire) *via* le prolongement des formes linéaires.

Orthogonalité, dual d'un quotient ($(E/F)^* \sim F^\circ$), un sev est tout ssi son orthogonal est nul (raisonnement par orthogonalité, exemple en calcul intégral). Exo : $(\ker f)^\circ = \mathrm{im}({}^t f)$. En dimension finie, dimension de l'orthogonal, rang de la transposée.

Grassmanniennes, $F \mapsto F^\circ$ est une bijection $\mathcal{G}_p(E) \to \mathcal{G}_{n-p}(E^*)$ (explicitation de la réciproque avec l'orthogonal à gauche).

2.3 Produit tensoriel d'espaces vectoriels

Définition par existence et unicité d'un ev qui transforme le bilinéaire en linéaire (si E et F sont des k-ev, il existe un k-ev G et une application bilinéaire $c : E \times F \to G$ tels que pour toute application k-bilinéaire $E \times F \to H$, il existe une unique application linéaire $G \to H$ qui fasse commuter le diagramme qu'on sait *via* c ; en outre, si G, c et G', c' sont deux comme ça, il existe un isomorphisme $\varphi : G \to G'$ tel que $c' = \varphi \circ c$). Preuve de l'unicité par propriété universelle (et le "unique" dans la partie existence) ; preuve constructive de l'existence en quotientant l'espace engendré par les couples par les relations de bilinéarité.

Notation $E \otimes F$ ou $E \otimes_k F$, tenseurs élémentaires $x \otimes y = c(x, y)$, ils engendrent $E \otimes F$.

Propriétés élémentaires : $E \otimes k \sim E$, $E \otimes F \sim F \otimes E$, $E \otimes (F \otimes G) \sim (E \otimes F) \otimes G$, $f : E \to E'$ et $g : F \to F'$ induisent $f \otimes g : E \otimes E' \to F \otimes F'$.

Aussi $(\bigoplus_i E_i) \otimes (\bigoplus_j F_j) \sim \bigoplus_{(i,j)} E_i \otimes F_j$. En particulier, base du produit à partir d'une base des facteurs. Corollaire : $\dim E \otimes F = dim E \times \dim F$. Corollaire encore : $E^* \otimes F \sim \mathrm{Hom}_k(E, F)$ si F est de dimension finie (exo : et sinon ?). Vision de la trace *via* cet isomorphisme : c'est $l \otimes x \mapsto l(x)$.

Exercice : isomorphisme canonique entre $E^* \otimes F^*$ et $(E \otimes F)^*$ en dimension finie. Exercice : loi de l'algèbre $\mathrm{Hom}_k(E, E)$ dans sa version $E^* \otimes E$ (c'est $(l \otimes x)(l' \otimes x') = l'(x)(l \otimes x')$). Exercice : $k[X, Y] \sim k[X] \otimes_k k[X]$. Exercices sur suites exactes et produit tensoriel. Exercice : changement de corps de base $E \otimes_k K$ si K est une extension de k.

Toute application r-linéaire $E \times \cdots \times E \to F$ se factorise en une application linéaire $T^r(E) \to F$. *Algèbre tensorielle* $T(E) = \bigoplus_{r \geq 0} T^r(E)$ d'un ev E. Propriété universelle : toute application linéaire de E dans une k-algèbre A se prolonge en un homomorphisme de k-algèbres $T(E) \to A$. Toute application linéaire $f : E \to F$ induit un unique homomorphisme de k-algèbres $T(f) : T(E) \to T(F)$. Base de $T^r(E)$ à partir d'une base de E ; la dimension est $\dim(E)^r$. Si E est de dimension finie n, on peut voir $T(E)$ comme algèbre de polynômes non commutatifs à n indéterminées.

2.4 Algèbres symétrique et extérieure d'un espace vectoriel

2.4.1 Algèbre symétrique

$S^r(E)$ est le quotient de $T^r(E)$ par le sev engendré par les $x_1 \otimes \cdots \otimes x_r - x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(r)}$ où $\sigma \in \mathfrak{S}_r$. Toute application r-linéaire symétrique $E \times \cdots \times E \to F$ se factorise en une application linéaire $S^r(E) \to F$. *Algèbre symétrique* $S(E) = \bigoplus_{r \geq 0} S^r(E)$ de l'ev E. Propriété universelle : toute application linéaire de E dans une k-algèbre commutative A se prolonge en un homomorphisme de k-algèbres $S(E) \to A$. Toute application linéaire $f : E \to F$ induit un unique homomorphisme de k-algèbres $S(f) : S(E) \to S(F)$.

Somme directe : $S^r(E \oplus E') \sim \bigoplus_{p+q=r} S^p(E) \otimes S^q(E)$, ou directement en termes d'algèbres graduées $S(E \oplus E') \sim S(E) \otimes S(E')$. Base de $S^r(E)$ à partir d'une base de E ; si $\dim(E) = n$, la dimension de $S^r(E)$ est $\binom{n+r-1}{r}$. En dimension finie, $S(E)$ est isomorphe à l'algèbre des polynômes à $\dim(E)$ indéterminées.

2.4.2 Algèbre extérieure, déterminants

$\Lambda^r(E)$ est le quotient de $T^r(E)$ par le sev engendré par les $x_1 \otimes \cdots \otimes x_r$ où au moins deux x_i sont égaux. Toute application r-linéaire alternée (nulle si deux coordonnées sont égales) $E \times \cdots \times E \to F$ se factorise en une application linéaire

$\Lambda^r(E) \to F$. *Algèbre extérieure* $\Lambda(E) = \bigoplus_{r\geq 0} \Lambda^r(E)$ de l'ev E. Propriété universelle en caractéristique différente de 2 : toute application linéaire de E dans une k-algèbre anti-commutative A (*i.e.* $xy = -yx$) se prolonge en un homomorphisme de k-algèbres $\Lambda(E) \to A$ (exercice : que se passe-t-il en caractéristique 2 ?). Toute application linéaire $f : E \to F$ induit un unique homomorphisme de k-algèbres $\Lambda(f) : \Lambda(E) \to \Lambda(F)$.

Somme directe : $\Lambda^r(E \oplus E') \sim \bigoplus_{p+q=r} \Lambda^p(E) \otimes \Lambda^q(E)$, ou directement en termes d'algèbres graduées $\Lambda(E \oplus E') \sim \Lambda(E) \otimes \Lambda(E')$. Base de $\Lambda^r(E)$ à partir d'une base de E ; la dimension est $\binom{n}{r}$.

En TD : déterminants, mineurs, grassmanniennes, ideaux de Fitting.

3 Corps commutatifs

3.1 Degré d'une extension

3.1.1 Degré

Si K est un sous-corps de L, on dit que L est une *extension* de K. Dans cette situation, L est un K-espace vectoriel. On note $[L : K] = \dim_K(L)$ (c'est un cardinal), c'est le *degré* de L sur K. Lorsque le degré est fini, on dit que l'extension est *finie*. Par exemple, l'extension $\mathbb{R} \subset \mathbb{C}$ est de degré 2, $\mathbb{Q} \subset \mathbb{Q}[i] = \{a + bi,\ a, b \in \mathbb{Q}\}$ est de degré 2 (exo : $\mathbb{Q}[i]$ est un corps), $\mathbb{Q} \subset \mathbb{R}$ est de degré infini, puissance du continu. Proposition : multiplicativité des degrés ; preuve et "base télescopique".

3.1.2 Corps des fractions d'un anneau intègre

Si A est un anneau intègre, le *corps des fractions* de A est $\mathrm{Fr}(A) = \{a/b,\ a \in A,\ b \in A \setminus (0)\}$, avec les lois ordinanires sur les fractions ; A est un sous-anneau de $\mathrm{Fr}(A)$. Construction formelle : relation d'équivalence sur $A \times A \setminus (0)$ définie par $(a, b) \sim (a', b') \Leftrightarrow ab' = a'b$ (la transitivité fait intervenir l'intégrité de A), compatible avec les lois $(a, b)+(a', b') = (ab'+a'b, bb')$ et $(a, b)(a', b') = (aa', bb')$; d'où la structure d'anneau sur l'ensemble quotient $\mathrm{Fr}(A)$, le zéro et l'unité sont les classes respectives de $(0, 1)$ et $(1, 1)$, l'opposé de $cl(a, b)$ est $cl(-a, b) = cl(a, -b)$, l'inverse de $cl(a, b)$ est $cl(b, a)$ si $a \neq 0$. Le plongement est l'homomorphisme injectif d'anneaux $A \to \mathrm{Fr}(A)$, $a \mapsto cl(a, 1)$. Propriété universelle : tout homomorphisme d'anneaux injectif $A \to K$ où K est un corps se prolonge en $\mathrm{Fr}(A) \to K$.

Exemples : $\mathbb{Q} = \mathrm{Fr}(\mathbb{Z})$ (définition de $\mathbb{Q}$). Corps $K(X)$ des fractions rationnelles sur un corps K : c'est $\mathrm{Fr}(K[X])$, quotients "formels" de polynômes. L'extension $K \subset K(X)$ est infinie (exo : base de $K(X)$ comme K-espace vectoriel). Exercice : si A est intègre, quel est le corps des fractions de $A[X]$?

3.1.3 Caractéristique d'un anneau

Si A est un anneau, définition de $n.a$ si $n \in \mathbb{Z}$ et $a \in A$. L'application $\chi : \mathbb{Z} \to A$, $n \mapsto n.1$ est un homomorphisme d'anneaux. La *caractéristique* de A, notée $\mathrm{car}(A)$ est 0 si χ est injectif, sinon le générateur positif du noyau de χ.

Proposition : la caractéristique d'un anneau intègre est zéro ou un nombre premier. En effet, χ se factorise en un homomorphisme injectif d'anneaux $\overline{\chi} : \mathbb{Z}/\ker(\chi) \to A$, donc $\mathbb{Z}/\ker(\chi)$ est intègre [énoncer la propriété universelle du quotient d'un anneau par un idéal ; preuve en exercice]. En particulier, la caractéristique d'un corps est 0 ou un nombre premier. Par exemple, $\mathrm{car}(\mathbb{C}) = \mathrm{car}(\mathbb{C}[X]) = \mathrm{car}(\mathbb{C}(X)) = 0$, $\mathrm{car}(\mathbb{Z}/p\mathbb{Z}) = \mathrm{car}(\mathbb{Z}/p\mathbb{Z}[X]) = \mathrm{car}(\mathbb{Z}/p\mathbb{Z}(X)) = p$. Exercice : un anneau de caractéristique nulle est infini. Exercice : dans un anneau de caractéristique première p, on a l'identité polynomiale $(X+Y)^p = X^p+Y^p$ et même $(X+Y)^{p^a} = X^{p^a}+Y^{p^a}$ $(a \in \mathbb{N})$. Exercice :

quelles formules de Taylor pour les polynômes en caractéristique p ? Exercice : un anneau de caractéristique première (resp. nulle) est-il nécessairement intègre ?

Définition du *sous-corps premier* d'un corps K : c'est $\overline{\chi}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$ si $\mathrm{car}(K) = p$, ou $\mathrm{Fr}(\overline{\chi}(Z)) \simeq \mathbb{Q}$ si $\mathrm{car}(K) = 0$. C'est le sous-corps minimum de K : si $\mathrm{car}(K) = p$ (resp $= 0$), K contient un unique sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (resp. $\mathbb{Q}$) ; c'est le sous-corps premier de K, contenu dans tous les sous-corps de K. Tout corps est un espace vectoriel sur son sous-corps premier. En particulier, le cardinal d'un corps fini est la puissance d'un nombre premier (il n'y a pas de corps à 15 éléments). Exercice : tout anneau intègre fini est un corps.

3.1.4 Sous-anneau engendré

Définition de sous-anneau (respectivement sous-corps) engendré par une partie.

Dans la situation A sous-anneau de B et $E \subseteq B$, on note $A[E]$ les sous-anneau de B engendré par $A \cup E$. Si $E = \{x_1, \ldots, x_n\}$ est fini, on note $A[x_1, \ldots, x_n]$ C'est alors l'image de la spécialisation (homomorphisme d'anneaux) $A[X_1, \ldots, X_n] \to B$.

Si L est une extension de K et E est une partie de L, on note $K(E)$ les sous-corps de L engendré par $K \cup E$. Si $E = \{x_1, \ldots, x_n\}$ est fini, on note $K(x_1, \ldots, x_n)$. Exercice : $K(x_1, \ldots, x_n) = \mathrm{Fr}(K[x_1, \ldots, x_n])$.

S'il existe $x \in L$ tel que $L = K(x)$, on dit que l'extension $K \subset L$ est *monogène*, et que x est un *élément primitif* de L sur K.

3.2 Dépendance algébrique

Définition de la *dépendance algébrique* d'une partie finie d'un anneau sur un sous-anneau. Cadre d'une extension de corps, définition d'*élément algébrique* ou *transcendant*. [Pour plus tard, définition d'*élément entier* d'un anneau sur un sous-anneau]. Un nombre complexe est dit *algébrique* (tout court) s'il est algébrique sur $\mathbb{Q}$, transcendant sinon ; il est dit *entier* s'il l'est sur $\mathbb{Z}$. Exemples : $\sqrt{2}$, i, $\exp(i\pi/14)$ sont algébriques ; on peut montrer que π et e sont transcendants (dur).

En TD, base et degré de transcendance.

Soit $K \subset L$ une extension, et $x \in L$. Soit $\delta_x : K[X] \to L$, $P \mapsto P(x)$; c'est un homomorphisme de K-algèbres (exo) dont l'image est $K[x]$. Son noyau est un idéal de $K[X]$ qui est principal (division euclidienne) et x est transcendant sur K si, et seulement si δ_x est injectif.

On suppose que x est algébrique. L'unique polynôme unitaire qui engendre $\ker \delta_x$ est appelé *polynôme minimal* de x ; on le notera μ_x. Par propriété universelle du quotient (pour les anneaux), δ_x se factorise en un isomorphisme d'anneaux $K[X]/(\mu_x) \xrightarrow{\sim} K[x]$. Comme $K[x]$ est un sous-anneau de L, il est intègre ; donc μ_x est irréductible sur K ; d'où $K[X]/(\mu_x)$ est un corps, et $K[x]$ aussi puisqu'il lui est isomorphe comme anneau.

Proposition. Soient $K \subset L$ une extension et $x \in L$. Lpssé : 1- x est algébrique sur K ; 2- $K[x]$ est un corps ; 3- $K[x] = K(x)$; 4- $\dim_K K[x]$ est finie. Dans ces

conditions, $\deg(\mu_x) = \dim_K K[x] = [K[x] : K]$.

Proposition. Soient $K \subset L$ une extension et $x \in L$. Lpssé : 1- x est transcendant sur K ; 2- $K[x] \simeq K[X]$; 3- $K(x) \simeq K(X)$; 4- $K[x] \neq K(x)$; 5- $\dim_K K[x]$ est infinie.

Définition d'extension algébrique. Toute extension finie est algébrique (réciproque fausse, voir ci-dessous).

Théorème *Si $K \subset L$ une extension, l'ensemble des éléments de L qui sont algébriques sur K est un sous-corps de L.*

Preuve par multiplicativité des degrés. Remarque sur la non constructivité de la preuve et la difficulté de trouver un polynôme annulateur. Définition de $\overline{\mathbb{Q}}$, corps des nombres algébriques. C'est une extension infinie et algébrique de $\mathbb{Q}$.

3.3 Corps de rupture, corps de décomposition

$P \in K[X]$, irréductible. Une extension L de K est un *corps de rupture* de P lorsque L contient une racine de P et est minimal pour cette propriété (*i.e.* L est engendré par K et cette racine) ; L est un *corps de décomposition* de P lorsque P est scindé dans L et L est minimal pour cette propriété (*i.e.* L est engendré par K et les racines de P dans L).

Théorème *$K[X]/(P)$ est un corps de rupture de P et tout corps de rupture de P lui est isomorphe.*

Preuve : P a la classe de X pour racine dans $K[X]/(P)$, et tout corps contenant une racine de P est extension de $K[X]/(P)$ par propriété universelle du quotient. Enfin, tout corps de rupture est extension de degré 1 de $K[X]/(P)$ par minimalité.

Remarques. 1- A cause de l'unicité, on parle "du" corps de rupture d'un polynôme irréductible. 2- L'extension $K \subset K[X]/(P)$ est monogène. 3- Le corps de rupture de X^2+1 sur $\mathbb{R}$ est $\mathbb{C}$ (définition de $\mathbb{C}$). C'est aussi un corps de décomposition de X^2+1. De même, le corps de rupture de X^2-2 sur $\mathbb{Q}$ est un corps de décomposition. 4- Sur $\mathbb{Q}[\sqrt[3]{2}]$, corps de rupture de X^3-2 sur $\mathbb{Q}$, le polynôme X^3-2 n'est pas scindé (car $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$, par exemple) : $\mathbb{Q}[\sqrt[3]{2}]$ n'est pas un corps de décomposition de X^3-2 sur $\mathbb{Q}$.

Théorème *Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près.*

Preuve. Existence par récurrence sur le degré : prendre un corps de rupture $K[x_1]$ (d'un facteur irréductible de P), écrire $P = (X-x_1)Q$ (division euclidienne), prendre un corps de décomposition $K[x_1][x_2, \ldots, x_n]$ de Q sur $K[x_1]$, il convient. Unicité : on prouve, par récurrence sur $[L : K]$, que tout isomorphisme $f : K \xrightarrow{\sim} K'$ se prolonge en un isomorphisme sur des corps de décomposition L de P sur K et L' de $f(P)$ sur K' ; l'hypothèse de récurrence s'applique aux extensions $K[x] \subset L$ et $K'[f(x)] \subset L'$ où x est racine de P dans L, les corps de rupture $K[x]$ et $K'[f(x)]$ étant isomorphes.

Exercice : définir une notion de corps de décomposition pour un polynôme non nécessairement irréductible, et montrer que ce dernier théorème est encore valide.

Exemple : le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$ est $\mathbb{Q}(\sqrt[3]{2}, \exp(2i\pi/3))$; c'est une extension de degré 6.

3.4 Clôture algébrique

Un corps K est dit *algébriquement clos* lorsque tout polynôme non constant de $K[X]$ admet au moins une racine. C'est équivalent à demander que tout polynôme non constant soit scindé, ou que les seuls irréductibles soient les polynômes de degré 1, ou encore que toute extension algébrique (ou finie) de K égale K.

$\mathbb{C}$ et $\overline{\mathbb{Q}}$ sont algébriquement clos.

Une *clôture algébrique* de K est une extension algébrique $K \subset L$ où L est algébriquement clos. On admet l'existence et l'unicité à isomorphisme près de clôtures algébriques. "La" clôture algébrique de K est souvent notée $\overline{K}$.

Théorème de prolongement des plongements *Soient K un corps, $K \subset L$ une extension finie de K et C un corps algébriquement clos. Tout plongement $K \to C$ se prolonge en un plongement $L \to C$. Le nombre de tels plongements est au plus $[L : K]$.*

Preuve. Il suffit de le montrer pour une extension monogène $L = K[x]$ (récurrence sur $[L : K]$). Soit $\sigma : K \to C$ un plongement et μ_x le polynôme minimal de x sur K. Soit enfin α une racine de $\sigma.\mu_x$ dans C. On prolonge σ à $K[X]$ par $\sigma(X) = \alpha$, puis à $K[X]/(\mu_x)$ par propriété universelle du quotient. On compose ce dernier prolongement avec le (K-)isomorphisme canonique entre $K[X]/(\mu_x)$ et $K[x]$ (faire un dessin, gros diagramme commutatif). L'assertion sur le nombre de plongements vient de ce que tout prolongement de σ à $K[x]$ envoie nécessairement x sur une racine de $\sigma.\mu_x$ (mettre cette assertion dans la récurrence) ; on montre en même temps que le nombre de ces plongements est le nombre de racines distinctes de P dans C.

3.5 Corps finis

On a vu que le cardinal d'un corps fini est de la forme p^n (tout corps fini est une extension finie de son sous corps premier isomorphe à $\mathbb{Z}/p\mathbb{Z}$).

Théorème *Soient p un nombre premier et $n \in \mathbb{N}^*$. On note $q = p^n$. Le corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$ est, à isomorphisme près, l'unique corps à q éléments.*

On note ce corps $\mathbb{F}_q$. Par exemple, $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$.

Preuve. On note $\mathbb{F}_q$ le corps de décomposition de $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$. Soit k l'ensemble des racines de $X^q - X$ dans $\mathbb{F}_q$. Les racines de $X^q - X$ étant simples (dérivé vaut -1), k a q éléments. Comme le Frobenius est un homomorphisme d'anneaux, k est un sous-corps de $\mathbb{F}_q$; donc il égale $\mathbb{F}_q$ par minimalité du corps de décomposition. Si K est un corps à q éléments, il est extension de degré n de son sous-corps premier (isomorphe à) $\mathbb{Z}/p\mathbb{Z}$ et tous ses éléments x sont racines de $X^q - X$ (car le groupe K^* est d'ordre $q - 1$). Donc K est isomorphe à une extension de $\mathbb{F}_q$, donc à $\mathbb{F}_q$ pour des raisons de cardinal.

Théorème *Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique.*
Preuve. Soit $N(d)$ le nombre d'éléments d'ordre d de $\mathbb{F}_q^*$. Si $N(d) \neq 0$, soit x d'ordre d. Alors, les éléments de $\langle x \rangle$ sont les racines de $X^d - 1$ (il y a au plus d telles racines) ; ainsi tout élément d'ordre d est-il générateur de $\langle x \rangle$. Donc $N(d) = \varphi(d)$ dès que $N(d) \neq 0$. Par ailleurs, $q - 1 = \sum_{d \leq q-1} N(d)$ ($\mathbb{F}_q^*$ est la réunion de ses éléments d'ordre $1, 2 \dots$) et $q - 1 = \sum_{d|q-1} \varphi(d)$ (formule d'Euler, partition de $\mathbb{Z}/(q-1)\mathbb{Z}$ en éléments d'ordre d). Par coincements d'entiers, $N(d) = \varphi(d)$ pour tout diviseur d de $q - 1$. En particulier, $N(q - 1) \neq 0$.

Remarque : la même preuve montre que tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.

Exercice : on note $\mathbb{F}_q^2$ les carrés de $\mathbb{F}_q$. Si $p = 2$, alors $\mathbb{F}_q^2 = \mathbb{F}_q$. Si $p \geq 3$, calculer le nombre de carrés de $\mathbb{F}_q$ en considérant la suite exacte induite par $x \mapsto x^2$. Montrer que $x \in \mathbb{F}_q^2$ ssi $x^{\frac{q-1}{2}} = 1$ (seconde suite exacte induite par $x \mapsto x^{\frac{q-1}{2}}$). En déduire que $-1 \in \mathbb{F}_q^2$ ssi $q \equiv 1$ [4].

3.6 Théorie de Galois élémentaire

Si L est une extension de K et C un corps, un *K-plongement* de L dans C est un homomorphisme d'anneaux $L \to C$ valant l'identité sur K.

Théorème *Soit K un corps fini ou de caractéristique nulle. Si $K \subset L$ est une extension finie et C une extension algébriquement close de K, le nombre de K-plongements $L \to C$ est $[L : K]$.*
Preuve. Lemme : sur un tel corps, les polynômes irréductibles n'ont que des racines simples dans les extensions où ils sont scindés (le Frobenius est surjectif pour les corps finis).

[Une extension L de K pour lequel cette propriété est vraie pour toute extension algébriquement close C de K est dite *séparable* ; toute extension d'un corps fini ou de caractéristique nulle est ainsi séparable.]

Théorème de l'élément primitif *Soit K un corps fini ou de caractéristique nulle. Toute extension finie L de K est monogène (i.e. il existe $x \in L$ tel que $L = K[x]$).*
Preuve. On note $n = [L : K]$; alors, $x \in L$ est élément primitif ssi $1, x, \dots, x^{n-1}$ sont K-linéairement indépendants sur K. Soient $\sigma_1, \dots, \sigma_n$ les K-plongements de L dans une extension algébriquement close donnée C. Ssi $\sum_{1 \leq i \leq n} \lambda_i x^{i-1} = 0$ est une relation K-linéaire entre les x^i, alors les λ_i sont solutions du système linéaire homogène $\sum_{1 \leq i \leq n} \lambda_i \sigma_j(x)^{i-1} = 0$, $1 \leq j \leq n$. Le déterminant de ce système est un Vandermonde : x est primitif ssi les $\sigma_j(x)$ sont tous distincts, *i.e.* ssi x est hors de la réunion finie des noyaux des $\sigma_i - \sigma_j$. Dans le cas où K est infini, L n'est pas une réunion finie de sous-K-ev propres ; donc il existe un élément primitif. Dans le cas où K est fini, L l'est aussi et si x est un générateur du groupe multiplicatif $L^\times$, on a clairement $L = K[x]$.

Si L et L' sont deux extensions de K, un *K-isomorphisme* de L sur L' est un isomorphisme $L \to L'$ valant l'identité sur K ; dans ces conditions, on dit que L et L' sont des *corps conjugués sur K*. Un *K-automorphisme* de L est un K-isomorphisme $L \to L$. Les K-automorphismes $L \to L$ forment une groupe pour la composition ; on le note $\mathrm{Aut}_K(L)$.

Si L et L' sont deux extensions de K, $x \in L$, $x' \in L'$, on dit que x et x' sont *conjugués* lorsqu'il existe un K-isomorphisme $f : K[x] \to K[x]'$ tel que $f(x) = x'$ (f est alors unique). Cela signifie que x et x' sont tous les deux transcendants sur K, ou bien sont tous les deux algébriques et ont le même polynôme minimal sur K.

Si G est un sous-groupe de $\mathrm{Aut}_K(L)$, on note L^G le sous-corps de L des invariants sous G : $L^G = \{x \in L,\ \forall \sigma \in G,\ \sigma(x) = x\}$.

Théorème *Soient K un corps fini ou de caractéristique nulle et $K \subset L$ une extension finie. Lpssé.*

1- $K = L^{\mathrm{Aut}_K(L)}$;

2- pour tout $x \in L$, μ_x est scindé dans L ;

3- L est le corps de décomposition d'un polynôme sur K.

Dans ces conditions, $[L : K] = |\mathrm{Aut}_K(L)|$.

Preuve. $(1 \Rightarrow 2)$ $P = \prod_{s \in \mathrm{Aut}_K(L)}(X - s(x))$ est invariant par tout K-automorphisme de L, donc est dans $K[X]$; comme x l'annule, μ_x divise P, donc est scindé dans L. $(2 \Rightarrow 3)$ Si $L = K[x]$ (théorème de l'élément primitif), L est le corps de décomposition de μ_x sur K puisque μ_x est scindé sur L. $(3 \Rightarrow 1)$ Si $L = K[x]$ est le corps de décomposition de μ_x (toujours possible par le théorème de l'élément primitif), L a exactement $n = [L : K]$ K-automorphismes (envoyer x sur une racine de μ_x) ; si $y \in L^{\mathrm{Aut}_K(L)}$, tout K-automorphisme de L est aussi un $K[y]$-automorphisme de L. Ainsi, L admet-il au moins n $K[y]$-plongements dans une extension algébriquement close de L ; par le théorème de prolongement des plongements, cela entraîne que $[L : K[y]] \geq n$. Donc $K = K[y]$ (l'extension $K \subset K[y]$ est de degré 1). On a montré en passant que $[L : K] = |\mathrm{Aut}_K(L)|$ (les K-plongements de L sont tous des K-automorphismes).

[Une extension L de K telle que tout K-plongement $\sigma : L \to C$ dans une extension C de L vérifie $\sigma(L) \subset L$ est dite *normale*. Par exemple, les corps de décomposition sont des extensions normales.]

Une extension qui vérifie les conditions de ce théorème est dite *galoisienne* (une extension est galoisienne lorsqu'elle est à la fois normale et séparable). Le groupe $\mathrm{Aut}_K(L)$ est alors appelé *groupe de Galois* de L. On le notera parfois $\mathrm{Gal}(L/K)$.

Corollaire. *$K \subset L$ finie. Si H est un sous-groupe de $\mathrm{Aut}_K(L)$ tel que $K = L^H$, alors l'extension $K \subset L$ est galoisienne et $H = \mathrm{Gal}(L/K)$.*

Preuve. Si $x \in L$, le polynôme $\prod_{s \in H}(X - s(x)) \in K[X]$ est multiple de μ_x : ce dernier est scindé. Donc l'extension est galoisienne. Si en outre x est élément primitif, $|\mathrm{Gal}(L/K)| = [L : K] = \deg(\mu_x) \leq |H| \leq |\mathrm{Gal}(L/K)|$; d'où l'égalité.

Si $K \subset L$ est une extension galoisienne, on a une correspondance

$$\begin{array}{ccc} \{sous-groupes\ de\ \mathrm{Gal}(L/K)\} & \to & \{sous-extensions\ K \subset F \subset L\} \\ G & \to & L^G \\ \mathrm{Aut}_F(L) & \leftarrow & F \end{array}$$

Théorème (correspondance de Galois) *Soit $K \subset L$ une extension galoisienne.*

1- Si $K \subset F \subset L$ est une sous-extension, l'extension $F \subset L$ est galoisienne et les deux applications ci dessus $G \mapsto L^G$ et $F \mapsto \mathrm{Gal}(L/F)$ sont des bijections réciproques, décroissantes pour l'inclusion.

2- Si $K \subset F \subset L$ est une sous-extension, l'extension $K \subset F$ est galoisienne si, et seulement si $\mathrm{Gal}(L/F) \lhd \mathrm{Gal}(L/K)$. Dans ces conditions, la restriction des K-automorphismes de L induit un isomorphisme de groupes

$$\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F).$$

Preuve. 1- Si $x \in L$, $\mu_{x,F}$ divise $\mu_{x,K}$ qui est scindé dès que L/K est galoisienne ; ainsi pour toute sous-extension F, L/F est-elle galoisienne. D'où $F = L^{\mathrm{Gal}(L/F)}$; si on note $k : G \mapsto L^G$ et $g : F \mapsto \mathrm{Gal}(L/F)$, cela montre que $k \circ g = \mathrm{id}$. Si G est un sous-groupe de $\mathrm{Gal}(L/K)$ et si $F = L^G$, alors $G = \mathrm{Gal}(L/F)$ (*i.e.* $G = \mathrm{Gal}(L/L^G)$) d'après le corollaire ci-dessus appliqué à l'extension L/F ; d'où $g \circ k = \mathrm{id}$. La décroissance de g et k est évidente. 2- Une sous-extension F/K est galoisienne ssi $\forall x \in F$, μ_x est scindé dans F, c'est-à-dire ssi $\forall x \in F$, $\forall \sigma \in \mathrm{Gal}(L/K)$, $\sigma(x) \in F$, ou encore ssi $\forall \sigma \in \mathrm{Gal}(L/K)$, $\sigma(F) \subseteq F$. Si $G \lhd \mathrm{Gal}(L/K)$ et si $F = L^G$, soient $x \in F$ et $\sigma \in \mathrm{Gal}(L/K)$; pour tout $\tau \in G = \mathrm{Gal}(L/F)$, on a $\tau\sigma(x) = \sigma\tau'(x) = \sigma(x)$ pour un certain $\tau' \in G$; ainsi $\sigma(x)$ est-il invariant par G : il est dans F, et l'extension F/K est galoisienne. Si F/L est galoisienne, soit $G = \mathrm{Gal}(L/F)$; pour tous $\tau \in G$, $\sigma \in \mathrm{Gal}(L/K)$ et $x \in F$, puisque $\sigma(x) \in F$, on a $\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\sigma(x) = x$: puisqu'il fixe F, $\sigma^{-1}\tau\sigma$ est dans G et G est normal. 3- Si F/K est galoisienne, le noyau de la restriction (alors bien définie) $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ est $\mathrm{Gal}(F/K)$. Pour des raisons de cardinaux finis, cela implique la surjectivité de l'homomorphisme induit sur le quotient.

Exemple. Soient $K = \mathbb{Q}$ et $L = \mathbb{Q}[j, \sqrt[3]{2}]$, corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. L'extension $L/\mathbb{Q}$ est galoisienne et de degré 6. Comme la sous-extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ n'est pas galoisienne (le polynôme minimal de $\sqrt[3]{2}$ n'y est pas scindé), le groupe $\mathrm{Gal}(L/\mathbb{Q})$ n'est pas abélien. Comme il est d'ordre 6, il est isomorphe à $\mathfrak{S}_3$. Etablir la liste des sous-groupes de $\mathrm{Gal}(L/\mathbb{Q})$ (ils sont cycliques, engendrés respectivement par $\sigma : (j, \sqrt[3]{2}) \mapsto (j, j\sqrt[3]{2})$, $\tau : (j, \sqrt[3]{2}) \mapsto (j^2, \sqrt[3]{2})$, et les deux conjugués de τ par σ et σ^2), celle des sous-extensions de L ($\mathbb{Q}[j]$, $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[j\sqrt[3]{2}]$ et $\mathbb{Q}[j^2\sqrt[3]{2}]$) et expliciter la correspondance de Galois.

3.7 Cyclotomie

Le n-ième polynôme cyclotomique (rationnel) est $C_n = \prod_\zeta (X - \zeta)$, le produit portant sur les racines primitives n-ièmes complexes de l'unité. Son degré est $\varphi(n)$ (Euler).

Comme les racines primitives n-ièmes sont les éléments d'ordre n du groupe cyclique des racines n-ièmes, on a la formule $X^n - 1 = \prod_{d|n} C_d$ qui permet le calcul des C_n et de montrer que $C_n \in \mathbb{Z}[X]$. Exemple des premiers calculs (jusqu'à C_{10}).

Théorème de Wedderburn *Tout corps fini est commutatif*

Théorème *Les polynômes cyclotomiques sont irréductibles dans* $\mathbb{Z}[X]$.

Voir Perrin pour des preuves.

Comme C_n est scindé sur $\mathbb{Q}[\zeta_n]$ (où ζ_n est n'importe quelle racine primitive n-ièmes de l'unité), l'extension $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ est galoisienne. On note $G_n = \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$, groupe d'ordre $\varphi(n)$. Tout élément σ de G_n est déterminé par l'image $\sigma(\zeta_n)$, qui est une puissance $\zeta_n^{k(\sigma)}$. L'application $k : G_n \to (\mathbb{Z}/n\mathbb{Z})^\times$ est un homomorphisme injectif de groupes ; pour des raisons de cardinal fini, c'est un isomorphisme. Ainsi, $\boxed{G_n \simeq (\mathbb{Z}/n\mathbb{Z})^\times}$.

Par ailleurs, si $n = \prod_i p_i^{a_i}$, le théorème chinois assure que $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_i (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$, et on a les résultats suivants (voir Perrin par exemple).

Théorème $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$ *et si* $a \geq 2$, *alors* $(\mathbb{Z}/2^a\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{a-2}\mathbb{Z}$. *Si* p *est un nombre premier* $\neq 2$ *et* $a \geq 1$, *alors* $(\mathbb{Z}/p^a\mathbb{Z})^\times \simeq \mathbb{Z}/p^{a-1}(p-1)\mathbb{Z}$;

3.8 Norme, trace et discriminant dans les corps de nombres

En TD.

3.9 Corps quadratiques

En TD.

3.10 Constructions à la règle et au compas

En TD.

3.11 Equations polynomiales

En TD.

4 Appendice : axiomatiques des structures abstraites de groupes, anneaux, corps, espaces vectoriels, modules et algèbres

4.1 Groupes

4.1.1 Définition, axiomes

Un **groupe** est un ensemble G muni d'une *loi de composition interne* notée ici $\times$ (*i.e.* une application $G \times G \to G$, $(x, y) \mapsto x \times y$) vérifiant les trois axiomes suivants :

1- la loi $\times$ est *associative (i.e.* $(x \times y) \times z = x \times (y \times z)$ pour tous x, y, et z de G ; on note $x \times y \times z$ ce produit) ;

2- G possède un *élément neutre* e pour $\times$ (*i.e.* $x \times e = e \times x = x$ pour tout $x \in G$; on note souvent 1 l'élément neutre) ;

3- tout élément de G possède un *symétrique* pour $\times$ (*i.e.* pour tout $x \in G$, il existe $y \in G$ tel que $x \times y = y \times x = e$; on note souvent $y = x^{-1}$).

Si en outre $\times$ est *commutative* (*i.e.* $x \times y = y \times x$ pour tous x et y de G), le groupe est dit *commutatif* ou *abélien*.

On omet souvent le symbole $\times$ de la loi en notant $xy = x \times y$. On note parfois $+$ la loi des groupes commutatifs ; dans ces conditions, l'élément neutre est noté 0 et le symétrique de tout $x \in G$ est noté $-x$.

4.1.2 Sous-groupe, homomorphisme de groupes

Un **sous-groupe** d'un groupe G est une partie de G qui soit un groupe pour la loi de G.

Proposition *Une partie non vide H d'un groupe G est un sous-groupe de G si, et seulement si :*

1- H est stable pour la loi de G (i.e. $x \times y \in H$ pour tous x et y de H) ;

2- le symétrique (pour la loi de G) de tout élément de H est dans H.

Un **homomorphisme de groupes** est une application f d'un groupe G dans un groupe G' qui préserve les lois de G et de G', c'est-à-dire telle que $f(xy) = f(x)f(y)$ pour tous x et y de G.

4.1.3 Exemples fondamentaux

L'addition usuelle dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{Z}$, et dans leurs puissances.

La multiplication usuelle dans $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{R}_+^*$ ou $\mathbb{C}^*$, dans l'ensemble des nombres complexes de module un, dans l'ensemble des racines n-ièmes de l'unité ($n \geq 1$) et dans l'ensemble de toutes les racines de l'unité.

La composition dans le groupe symétrique ; dans le groupe linéaire $\mathrm{GL}(E)$ d'un espace vectoriel E et dans ses sous-groupes $\mathrm{SL}(E)$, $\mathrm{O}(E)$, $\mathrm{SO}(E)$, $\mathrm{U}(E)$, $\mathrm{SU}(E)$; dans l'ensemble des similitudes (resp. des similitudes directes) vectorielles d'un espace euclidien ; dans $\mathrm{GA}(E)$ (groupe affine de l'espace affine E) et dans ses sous-groupes des translations, des homothéties-translations, des isométries, des rotations, des similitudes etc...

Le produit matriciel dans $\mathrm{GL}_n(A)$ (matrices carrées $n \times n$ inversibles à coefficients dans l'anneau A), $\mathrm{SL}_n(A)$, $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$, $\mathrm{U}_n(\mathbb{C})$, $\mathrm{SU}_n(\mathbb{C})$; dans l'ensemble des matrices triangulaires supérieures (resp. inférieures) inversibles, dans l'ensemble des matrices diagonales inversibles, etc...

Plus généralement, les groupes d'automorphismes (structures algébriques, topologiques, géométriques, *etc*).

4.2 Anneaux

4.2.1 Définition, axiomes

Un **anneau** (unitaire) est un ensemble A muni de deux lois de composition interne notées ici $+$ (addition) et $\times$ (multiplication) vérifiant les axiomes suivants :

1- $(A, +)$ est un groupe abélien ; on note souvent son élément neutre 0 et $-a$ le symétrique de $a \in A$ pour $+$ (on parle de l'*opposé* de a) ;

2- la loi $\times$ est associative et admet un élément neutre souvent noté 1 ;

3- la multiplication est *distributive* par rapport à l'addition (*i.e.* $a \times (b + c) = (a \times b) + (a \times c)$ et $(a + b) \times c = (a \times c) + (b \times c)$ pour tous a, b et c de A).

Si en outre la multiplication est commutative, l'anneau est dit *commutatif*.

Les règles de calcul dans un anneau commutatif sont celles de $\mathbb{Z}$; en particulier, la formule du binôme de Newton est vraie dans un anneau commutatif (ou dans un anneau général entre deux éléments qui commutent). Dans les systèmes de parenthésages, on donne la priorité à la multiplication ; ainsi, $a \times b + c = (a \times b) + c$.

4.2.2 Sous-anneau, idéal, homomorphisme d'anneaux

Un **sous-anneau** d'un anneau A est une partie de A qui soit un anneau pour les lois de A. Une partie B d'un anneau $(A, +, \times)$ est un sous-anneau de A si, et seulement si $(B, +)$ est un sous-groupe de $(A, +)$ contenant 1, et B est stable pour la multiplication de A.

Un **idéal** d'un anneau commutatif A est une partie I de A telle $(I, +)$ soit un sous-groupe de $(A, +)$ et $ia \in I$ pour tous $i \in I$ et $a \in A$.

Une application f d'un anneau A dans un anneau B est un **homomorphisme d'anneaux** si, et seulement si elle préserve les unités et les lois de A et B, c'est-à-dire si, et seulement si $f(1) = 1$, $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ pour tous x et y de A.

4.2.3 Exemples fondamentaux

Pour leurs lois usuelles, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ pour $n \geq 2$, les corps de nombres $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, l'ensemble des nombres décimaux (plus généralement, les localisés de $\mathbb{Z}$), les anneaux d'entiers d'extensions algébriques.

Les anneaux de polynômes à coefficients dans un anneau A.

Les anneaux de séries formelles.

L'anneau des endomorphismes d'un espace vectoriel (la multiplication est la composition), l'anneau des matrices carrées à coefficients dans un anneau (la multiplication est le produit matriciel).

L'ensemble des applications d'un ensemble E dans un anneau A (pour les lois usuelles $(f+g)(x) = f(x)+g(x)$ et $(fg)(x) = f(x)g(x)$) et ses sous-anneaux selon les structures (algébriques, topologiques, géométriques, *etc*) de E et A.

4.3 Corps

4.3.1 Définition, axiomes

Un **corps** est un anneau A dans lequel tout élément non nul x admet un symétrique pour la multiplication (on parle alors de l'*inverse* de x, souvent noté x^{-1}). Cela revient à demander que $A \setminus \{0\}$ soit un groupe pour la multiplication.

4.3.2 Sous-corps, plongements

Un **sous-corps** d'un corps L est une partie K de L qui soit un corps pour les lois de L. Cela revient à demander que $(K, +)$ soit un sous-groupe de $(L, +)$ et que $(K \setminus \{0\}, \times)$ soit un sous-groupe de $(L \setminus \{0\}, \times)$.

Un homomorphisme d'anneaux $k \to A$ où k est un corps est toujours injectif. On parle de **plongement** de k dans A ou d'**extension** de k.

4.3.3 Exemples fondamentaux

$\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ pour leurs lois usuelles. Les corps de nombres algébriques, le corps des nombres algébriques.

$\mathbb{Z}/p\mathbb{Z}$ si p est un nombre premier, les corps finis $\mathbb{F}_{p^a}$.

$k[X]/(P)$ si k est un corps et si P est un polynôme irréductible de $k[X]$; plus généralement, le quotient d'un anneau par un idéal maximal.

Les corps de fractions rationnelles sur un corps ; plus généralement, les corps de fractions des anneaux intègres.

Les sous-corps d'invariants par groupes d'automorphismes.

L'ensemble des fonctions méromorphes sur un ouvert de $\mathbb{C}$.

Le corps des quaternions (non commutatif) ; plus généralement, les corps de matrices.

Le corps des séries de Laurent, celui des séries de Laurent tordues (non commutatif).

4.4 Modules

4.4.1 Définition, axiomes

Un **module** sur l'anneau commutatif A est un ensemble M muni d'une loi de composition interne (*addition*) notée $+$ et d'une loi externe sur A notée $.$ (*i.e.* une application $A \times M \to M$, $(a, x) \mapsto a.x$, *multiplication par les scalaires*) vérifiant :

1- $(M, +)$ est une groupe abélien ;

2- pour tous $(a, b) \in A^2$ et $(x, y) \in M^2$,

- $1.x = x$;
- $(a + b).x = a.x + b.x$;
- $a.(x + y) = a.x + a.y$;
- $a.(b.x) = (ab).x$.

4.4.2 Sous-module, application linéaire

Un **sous-module** d'un A-module M est une partie de M qui soit un A-module pour les lois de M. Une partie N d'un A-module M est un sous-module de M si, et seulement si N est non vide et stable pour les lois de M, *i.e.* $x + y \in N$ et $a.x \in N$ pour tous $(x, y) \in N^2$ et $a \in A$.

Une application f d'un A-module M dans un A-module N est une application linéaire (ou homomorphisme de A-modules) si, et seulement si elle préserve les lois de M et N, c'est-à-dire si, et seulement si $f(x + y) = f(x) + f(y)$ et $f(a.x) = a.f(x)$ pour tous $(x, y) \in M^2$ et $a \in A$.

4.4.3 Exemples fondamentaux

A^n où $n \in \mathbb{N}^*$, pour les lois $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ et $a.(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$; plus généralement, les A-modules libres.

Les $\mathbb{Z}$-modules sont les groupes abéliens.

Si u est un endomorphisme d'un A-module M, la loi externe $P.x = P(u)(x)$ fait de M un $A[X]$-module. Dans le cas où A est un corps, c'est un cadre naturel pour la réduction de l'endomorphisme u.

Les idéaux d'un anneau commutatif.

Si $f : A \to B$ est un homomorphisme d'anneaux, B est un A-module pour son addition et la loi externe $a.b = f(a) \times b$.

L'ensemble des applications linéaires d'un A-module dans un autre (pour les lois $(f + g)(x) = f(x) + g(x)$ et $(a.f)(x) = a.f(x)$), notamment les formes linéaires (module dual). Plus généralement, l'ensemble des applications d'un ensemble dans un A-module pour les lois usuelles.

4.5 Espaces vectoriels

4.5.1 Définition, axiomes

Un **espace vectoriel** sur le corps k est un k-module.

4.5.2 Sous-espace vectoriel, application linéaire

Un **sous-espace vectoriel** d'un espace vectoriel E est une partie de E qui soit un espace vectoriel pour les lois de E. Une partie F d'un espace vectoriel E en est un sous-espace vectoriel si, et seulement si F est non vide et stable pour les lois de E.

Une **application k-linéaire** d'un k-espace vectoriel E sur un k-espace vectoriel F est un homomorphisme de k-modules.

4.5.3 Exemples fondamentaux

k^n où $n \in \mathbb{N}^*$, pour les lois usuelles ; prototype d'espace vectoriel de dimension finie égale à n ; plus généralement l'ensemble des fonctions d'un ensemble E dans un k-espace vectoriel pour les lois usuelles (la dimension est le cardinal de E).

Si A est un anneau, extension d'un corps k, alors A est un espace vectoriel sur k (d'où les cardinaux des corps finis).

4.6 Algèbres

4.6.1 Définition, axiomes

Une **algèbre** (unifère) sur l'anneau A est un ensemble B muni de deux lois de composition interne notées $+$ (*addition)* et $\times$ (*multiplication*) et d'une loi externe sur A notée . (*multiplication par les scalaires*) vérifiant :

1- $(B, +, \times)$ est un anneau ;

2- $(B, +, .)$ est un A-module ;

3- $(a.x) \times y = x \times (a.y) = a.(x \times y)$ pour tous $(x, y) \in B$ et $a \in A$; on note ce produit $a.x \times y$.

L'axiome **3-** revient à demander que l'application $B \times B \to B$, $(x, y) \mapsto x \times y$ soit bilinéaire pour la structure de A-module de B. L'image de l'application $A \to B$, $a \mapsto a.1_B$ est contenue dans le centre de B ; on trouve parfois ce dernier point de vue pour définir les algèbres.

Lorsque l'anneau $(B, +, \times)$ est commutatif, on dit que l'algèbre est commutative.

4.6.2 Sous-algèbre, homomorphisme d'algèbres

Une partie d'une algèbre en est une **sous-algèbre** lorsqu'elle en est à la fois un sous-anneau et un sous-module. Les sous-algèbres sont les sous-anneaux stables pour la loi externe.

Une application d'une A-algèbre dans une autre est un **homomorphisme de A-algèbres** si, et seulement si elle est à la fois une application linéaire et un homomorphisme d'anneaux.

4.6.3 Exemples fondamentaux

L'ensemble des endomorphismes d'un module (la multiplication est la composition).

L'ensemble des matrices carrées à coefficients dans un anneau (la multiplication est le produit matriciel).

Les $\mathbb{Z}$-algèbres sont les anneaux.

Les algèbres de polynômes à coefficients dans un anneau.

L'ensemble des applications d'un ensemble dans une A-algèbre.

L'algèbre d'un groupe sur un anneau (un corps, souvent). Elle est commutative en même temps que le groupe.

Les algèbres tensorielle, symétrique et extérieure d'un A-module (d'un k-espace vectoriel, souvent).

Si $A \to B$ est un homomorphisme d'anneaux, la structure de A-module qu'il induit sur B en fait une A-algèbre.