**Chapitre 12. Corps**

Un **anneau** **non-unitaire** correspond à un la donnée de tels que groupe commutatif de neutre et l.c.i. associative sur et distributive a gauche et a droite par rapport a .

Un **anneau = anneau unitaire** correspond à un la donnée de tel que anneau et élément neutre pour la multiplication.

Un **anneau commutatif** est un anneau dans lequel est commutatif  
Un anneau non nul est **intègre** ssi ou

On note l’ensemble des éléments inversibles d’un anneau. On note   
Un **sous-anneau** d’un anneau est une partie non vide de qui est encore un anneau pour les lois induites et qui contient le neutre multiplicatif de . Autrement dit c’est une partie telle que . (entraine automatiquement )  
Un **morphisme d’anneaux (unitaires)** est une application entre deux anneaux telle que

Un **corps** est un anneau unitaire commutatif dans lequel tout élément non nul est inversible .  
Un **morphisme de corps** est une application entre deux corps telle que on a alors  
Un morphisme de corps est donc un morphisme d’anneaux unitaires.  
On dit que  **est un espace vectoriel** ssi est un corps, est un groupe abélien, est une l.c.e. sur , et pour tous on a   
**Un morphisme d’evs**, d’un ev vers un ev sur le même corps est une application telle que et , càd telle que

On dit que  **est une -algèbre (unitaire)** ssi est un -espace vectoriel, est un anneau (unitaire), et pour tous

Une **-sous-algèbre** d’une -algèbre est une partie non vide de , telle que / , et qui munie des lois induites est encore une -algèbre.  
**Caractérisation sous-algèbre.** Une partie d’une -algèbre , est une **-sous-algèbre** de

ssi est un sous-anneau unitaire de et -sev de

ssi et

On a donc (dans le cas unitaire) .  
Un **morphisme d’algèbres**, d’une -algèbre vers une-algèbre sur le même corps est à la fois un morphisme d’anneau et un morphisme d’espaces vectoriels de vers càd que c’est une application telle que .  
**Séries formelles.** On note un ensemble quelconque d’indéterminées.  
Une **série formelle d’indéterminées sur un anneau commutatif** correspond à un élément . On note , la série formelle correspondant a .  
On note l’ensemble des séries formelles d’indéterminées sur un anneau commutatif .  
On définit   
On définit   
 est un anneau commutatif unitaire, avec , de .  
**Polynômes.**  
Un **polynôme d’indéterminées sur un anneau commutatif**  correspond à une série formelle , donc à un , tel que est fini.  
On note l’ensemble des polynômes formels d’indéterminées sur .  
 est un anneau commutatif unitaire, avec .  
Soit un corps, et un sur-corps de .  
Pour , et , on note l’évaluation de en .  
On note   
On note , **la** **fonction polynomiale sur** .   
On note , **le** **morphisme d’évaluation en un point** .  
On note , **la fonctionnalisation polynômiale dans** .  
La fonctionnalisation polynomiale est un morphisme de -algèbres.  
Le morphisme d’évaluation en un point est un morphisme de -algèbres.  
**Fractions rationnelles.**  
Pour un corps , est un anneau intègre.  
Pour un corps ,   
Pour un corps , est un corps.  
Soit un corps, et un sur-corps de .  
L’ensemble de définition d’une fraction dans est   
Pour , et , on note l’évaluation de en .  
Pour , et , on note   
On note   
On note , **la** **fonction rationnelle** .   
On note , **le** **morphisme d’évaluation en** .  
On note , **la fonctionnalisation rationnelle**.  
La fonctionnalisation rationnelle est un morphisme de -algèbres.  
Le morphisme d’évaluation en un point est un morphisme de -algèbres. **I. Extensions de corps**Un morphisme de corps est non nul et injectif.  
Un morphisme d’anneaux d’un corps vers un anneau est soit nul soit injectif.Pour un corps , il existe un unique morphisme d’anneaux tel que   
On a , la **caractéristique du corps**  est le générateur positif de qui est un idéal de donc un pour un unique qui s’avère être le plus petit tel que   
La caractéristique d’un corps est soit nulle, soit un nombre premier.   
Le morphisme est injectif ssi la caracteristique de est nulle.  
Dans ce cas se prolonge en un morphisme de corps   
 est un corps ssi c’est un anneau intègre ssi est premier.  
Un sous-groupe fini du groupe multiplicatif d’un corps est cyclique.  
Pour avec premier, le groupe est cyclique, ce qui n’était pas évident a priori.  
Un **sous-corps d’un corps**  correspond à une partie de qui muni des lois induites est un corps.  
L’intersection de sous-corps , est un sous-corps de   
**Le** **sous-corps engendré par une partie d’un corps** , est le plus petit sous-corps de qui contient . On le note **.**  
Un **sur-corps d’un corps**  correspond à un corps , dont est un sous-corps.Une **extension d’un corps** correspond à un couple où est un corps et un morphisme de corps injectif de dans . est un isomorphisme de corps, donc on identifie généralement et , et on identifie a l’inclusion .  
Pour cette raison, on identifie généralement sur-corps et extension de corps.  
Cependant, certaines constructions d'extensions ne sont pas naturellement des sur-corps (par exemple le corps de rupture) et la définition d'extension ci-dessus permet plus de souplesse.  
On note un sur-corps/extension de corps . On n’explicite généralement pas , on considère .Toute extension d’un corps est une algèbre. En particulier tout corps est une algèbre.   
Une **tour d’extensions**, est une suite croissante finie ou non d’extensions de corps, càd une suite croissante de sur-corps.  
**L’extension formelle engendrée par un ensemble sur un corps**  est l’ensemble des fractions rationnelles sur , d’indéterminées , càd . C’est une extension . **est** **sous-extension de**  ssi est un sous-corps de et un sur-corps de .  
Autrement dit ssi est une tour d’extensions de corps.  
On dit aussi que  **est corps intermédiaire entre et**   
On dit aussi que **est une sur-extension de** L’intersection de sous-extensions de , est une sous-extension de .On définit **la sous-extension de engendrée par une partie notée** comme la plus petite sous-extension de contenant , càd comme le plus petit sous-corps de contenant et , soit *.*  
est constitué des éléments de pouvant être obtenus à partir d'éléments de et de grâce à un nombre fini d'additions, de multiplications et d'inversions*.* Autrement dit .  
On obtient **en évaluant dans .**  
 est une tour d’extensions.  
Le corps est unique, mais attention le corps , en général dépend de .  
Par contre si, et alors . ne dépend donc pas du corps considéré dans une tour d’extension fixée.   
Une **extension est engendrée par une partie**  ssi càd ssi on l’obtient en évaluant dedans.  
 est une extension engendrée par sur car .  
Dans , pour , est engendrée par car car tour.  
Une **extension simple d’un corps**  est une extension de engendrée par un seul de ses éléments, donc correspond à avec extension , tels que .  
Dans une extension , pour , est une extension simple de .  
L’extension formelle engendrée par une unique indéterminée et un corps , càd est une extension simple de .   
Remarque : En théorie des corps il faut distinguer de . Bien que ce soient deux concepts légèrement distincts, ils se comportent souvent de la même façon. On écrit souvent seulement , ce qui prête a confusion avec le corps des fractions formelles, si on a , on interprétera comme signifiant (en général on utilise une minuscule grecque), si on a juste une indéterminée on écrit généralement une majuscule , et se réfère au corps des fractions, pas a .   
Pour partie d’une extension ,   
Pour partie d’une extension ,   
Pour parties d’une extension ,   
Pour parties d’une extension ,   
Un **corps est premier** ssi il n’a pas d’autre sous-corps que lui-même.  
 est un corps premier. Pour premier, est un corps premier.  
Le **sous-corps premier d’un corps** , est le plus petit sous-corps de c’est-à-dire . Il est premier.  
Le sous-corps premier d’un corps de caractéristique nulle, est isomorphe a .  
Le sous-corps premier d’un corps de caractéristique premier, est isomorphe a .  
Un corps est premier ssi il coïncide avec son sous-corps premier.  
Des corps d’une tour d’extensions, ont le même sous-corps premier.  
Attention il existe des corps finis avec un nombre non premier d’éléments.  
Un -**morphisme d’extensions de corps entre deux extensions et** est un morphisme d’anneaux de qui vaut l’identité sur . Un tel morphisme est toujours injectif.  
En fait, -morphisme d’extensions de corps ssi morphisme de -algebres de .  
Un -**endomorphisme d’une extension**  est un morphisme d’extensions de corpsde .  
Un -**automorphisme d’une extension**  est un -endomorphisme bijectif de .  
Vu dans , un -endomorphisme, n’est autre qu’un morphisme de corps .  
On note l’ensemble des automorphismes sur le corps . Pour , c’est un sous-groupe de le groupe des permutations de .  
**Algébricité et Transcendantalité dans une algèbre.**   
**Le morphisme d’évaluation polynomial en un point d’une -algèbre** : .  
On note (ou juste ) l’image de ce morphisme, et le noyau du morphisme.  
 est une sous-algèbre de appelée **sous-algèbre engendrée par** .  
 est un idéal (principal) de appelé **idéal annulateur de .**Le morphisme d’évaluation est un morphisme de -algèbres, surjectif dans par construction.  
Le **morphisme d’évaluation polynomial factorisé**  est un isomorphisme de -algèbres.  
**Le morphisme d’évaluation fractionnel en un point d’une -algebre** : .  
On note (ou juste ) l’image de ce morphisme. On a   
Le **morphisme d’évaluation fractionnel factorisé**  est un isomorphisme de -algèbres.  
Pour non constant, est un corps ssi est irréductible ssi idéal maximal.  
Pour non constant, est -algèbre de dimension dont est une base.  
 est une -algèbre de dimension infinie dont est une base.  
Un **élément d’une -algebre est transcendantal sur**  ssi   
Dans ce cas :   
 est -algèbre-isomorphe a . Donc , base de   
 est -algèbre-isomorphe a .  
Un **élément d’une -algebre est algébrique sur**  ssi   
Dans ce cas, le **polynôme minimal** d’un élément algébrique noté est l’unique polynôme de unitaire générant l’idéal annulateur de cet élément .   
Autrement dit, c’est l’unique polynôme annulateur de , unitaire de . On a donc   
Ainsi, être un polynôme annulateur de signifie être multiple du polynôme minimal.  
 est -algèbre-isomorphe a .  
Dans le cas algébrique on a .  
 est une base de avec .  
De plus, si est intègre, est irréductible sur et est un corps, et donc .   
Tout élément de s’écrit de façon unique comme un polynôme de degré   
**Caractérisation dans un anneau intègre:**  
 est algébrique ssi fini ssi fini ssi ssi ssi appartient à une extension finie de . Dans le cas contraire, est transcendant.  
**I.1. Nombres algébriques – Nombres transcendants.**  
Pour une extension de corps , on peut appliquer les définitions précédentes avec en voyant comme une -algebre, qui est aussi un anneau intègre.  
Un scalaire d’un corps est dit **algébrique sur un corps**  si c’est un zéro d’un polynôme non nul de   
Un scalaire d’un corps est **transcendant sur un corps**  s’il n’est pas zéro d’un polynôme non nul de   
Un **entier algébrique** est un zéro d’un polynôme unitaire (non nul) de .  
Un nombre algébrique (tout court) est un nombre algébrique sur . sont algébriques.  
 est transcendant, , sont transcendants.  
Si et sont algébriques (resp. entiers algébriques), alors aussi, et aussi.  
L’ensemble des entiers algébriques est un sous-anneau de .   
L’ensemble des nombres algébriques est un sous-corps de dénombrable.  
Donc il existe beaucoup de nombre transcendants car n’est pas dénombrable. **Une extension algébrique simple** est une extension simple avec algébriquesur .  
**Une extension transcendante simple** est extension simple avec transcendantsur .  
Plus généralement une **extension algébrique (resp. transcendante)** d’un corps est une extension dont tout est algébrique (resp. transcendant) sur .  
Pour une extension de corps , la somme, le produit, l’inverse par un non nul, ou le quotient par un non nul, d’éléments de algébriques sur , donne encore un élément de algébrique sur .  
La composée de deux extensions algébriques est algébrique.  
 algébrique de polynôme minimal . Si premier, algébrique de polynôme minimal   
**Nombre de Liouville.** Les réels avec sont transcendants.  
Le cardinal des réels transcendants est donc égal au cardinal de . **I.2. Extensions algébriques**Le polynôme minimal n’est défini que dans le cadre d’une extension de corps algébrique et est toujours irréductible, puisque est intègre.  
Pour algébrique, , est un corps, .  
Deux extensions algébriques simples qui admettent le même polynôme minimal sont isomorphes.  
Un morphisme d’extensions entre et qui envoie sur induit un isomorphisme entre les extensions simples , algebrique ssi algebrique et dans ce cas .Sur une extension algébrique, tout endomorphisme d’extension est bijectif, et donc un automorphisme. **I.3. Extensions transcendantes** est une extension transcendante simple.  
Toute extension transcendante simple est algèbre-isomorphe à l’extension .  
**I.4. Corps de rupture.**Un **corps de rupture d’un polynôme irréductible** est une extension simple dans laquelle est une racine de . De façon équivalente c’est une extension simple algèbrement-isomorphe au quotient . Un corps de rupture d’un polynôme irréductible est toujours un corps.  
Un polynôme irréductible sur admet toujours pour corps de rupture et celui-ci est unique a isomorphisme près (puisqu’ils y sont tous isomorphe). On choisira généralement par défaut.  
Une extension algébrique simple est toujours un corps de rupture de son polynôme minimal.  
Réciproquement, un corps de rupture est toujours une extension algébrique simple.  
Dans est irréductible, on pose une indéterminée, on pose le corps de rupture de , est donc un corps et dans , . est algébrique de polynôme minimal , donc est de dimension 2, . La somme ne change pas le degré donc se calcule comme la somme de polynômes , le produit dépassant le degré , doit passer au modulo : . On retrouve donc les lois usuelles de .  
Dans , on peut donc factoriser:   
Attention dans un corps de rupture , admet pour racine par construction, mais n’est pas forcement scindé dans .  
Exemple classique : sur le corps de rupture de P **II. Utilisation de l’algèbre linéaire  
II.1. Degré d’une extension**Pour toute extension de corps , alors est un .  
Le **degré d’une extension de corps**  noté est la dimension de en tant que ev.  
Pour une extension simple transcendante on a   
Pour une extension simple algébrique on a   
Pour deux extensions 2 corps successives on a   
Ainsi ssi ou   
Une **extension finie de corps**, est une extension de corps, de degré fini.  
Une extension finie de corps est toujours algébrique.  
Une extension algébrique simple est toujours finie.  
Cependant il existe des extensions algébriques (non simples) de degré infini. (TODO).  
Une extension de corps est finie ssi avec algébriques sur . **II.2. Construction à la règle et au compas**On se place dans on fixe un ensemble fini de points :  
On considère toutes les droites reliant 2 points de , et tous les cercles de centre un point de et de rayon une distance entre 2 points de .  
 est l’ensemble fini des points d’intersection entre 2 de ces droites, entre 2 de ces cercles, ou entre une de ces droites et un de ces cercles. On a donc construit   
On définit par récurrence , …, pour tout   
Un point de est **constructible** **à la règle (non graduée) et au compas** **en 1 étape à partir de** ssi .  
Un point de est **constructible à la règle et au compas à partir de (en un nombre fini d’étapes)** ssi   
Attention, dire un point est constructible en etapes ne signifie pas qu’il est dans .  
Un **nombre réel est constructible à la règle et au compas** ssi il est l’abscisse ou l’ordonnée d’un point de constructible a la règle et au compas en partant de .  
On note l’ensemble des réels constructibles à la règle et au compas.  
Un **polygone convexe est constructible à la règle et au compas** ssi ses sommets le sont en partant d’un ensemble formé de deux sommets adjacents.  
Un pentagone régulier est constructible à la règle et au compas.  
Une **famille** **séquentiellement** **constructible à la règle et au compas** **en étapes à partir de**  est une famille de points de telle que le point est constructible à la règle et au compas en 1 étape à partir de .  
Un point est **constructible en étapes** ssi il est le nième point d’une famille séquentiellement constructible.  
**Théorème de Wantzel, 1837.**  Soit une famille séquentiellement constructible à la règle et au compas en étapes à partir de , en notant le sous-corps de engendré par les coordonnées des points de de , alors on a pour tout ,   
, sont racines de polynômes de degré 2 a coefficients dans et le degré est 1 ou 2. Par multiplicativité des degrés est une puissance de 2  
**Réciproque Wantzel.** Soit une partie finie de , on pose le sous-corps de engendré par les coordonnées des points de . Soit une famille , de points de , on pose par récurrence . Si pour tout , est une extension de degré ou , alors la famille est séquentiellement constructible à la règle et au compas en étapes à partir de .  
**Théorème de Wantzel, version réelle.** L’ensemble des réels constructibles à la règle et au compas est un sous-corps de et donc une extension du sous-corps premier . Un réel est constructible ssi avec ssi le degré du polynôme minimal sur de est une puissance de 2.  
**Impossibilité de la duplication du cube.** On ne peut pas construire à la règle et au compas, le côté d’un cube de volume double du volume d’un cube de côté donné. Autrement dit, n’est pas constructible.  
**Impossibilité de la trisection d’un angle en général.** L’angle ne peut pas être divisé à la règle et au compas en trois angles égaux. Autrement dit n’est pas constructible.  
**Impossibilité de la quadrature du cercle.** On ne peut pas construire à la règle et au compas le côté d’un carré dont l’aire est égale à celle d’un disque donné. Autrement dit n’est pas constructible.  
**Impossibilité de la construction de l’heptagone régulier.** On ne peut pas construire à la règle et au compas, le côté d’un heptagone régulier. Autrement dit n’est pas constructible.  
L’ensemble des réels constructibles est stable par  **II.3. Corps de décomposition – Extensions normales – Extensions séparables**Un **corps de décomposition d’un polynôme non nul sur un corps** correspond à une extension de corps minimale pour l’inclusion qui rend scindé sur . Sur une telle extension, admet autant de racines que son degré et s’écrit , ce qui permet d’écrire l’extension   
Un corps de décomposition est une extension finie.  
 est un corps de décomposition de sur   
 est un corps de décomposition du -ieme polynome cyclotomique sur . (vérifier)  
 n’est pas un corps de décomposition de sur   
 est un corps de décomposition de sur .  
**Existence d’un corps de décomposition.** Un polynôme non nul sur un corps , admet toujours un corps de décomposition sur K.  
**Unicité a isomorphisme près du corps de décomposition.**   
Soit 2 corps isomorphes par l’isomorphisme , soit un polynôme non nul et sa version dans . Si est un corps de décomposition de , et est un corps de décomposition de , alors -isomorphes   
Un **corps est algébriquement clos** ssi tout polynôme est scindé sur lui autrement dit ssi tout polynôme de degré admet au moins une racine ssi il n’admet pas d’extension algébrique propre.  
**Une clôture algébrique d’un corps**  est une extension algébrique telle que est algébriquement clos.  
Une clôture algébrique de est un corps algébriquement clos minimal contenant , puisque si est un corps algébriquement clos contenant alors, parmi les éléments de , ceux qui sont algébriques sur forment une clôture algébrique de .  
Une clôture algébrique d’un corps a le même cardinal que si est infini ; elle est dénombrable si est fini.  
Souvent entre deux clôtures algébriques de il n’y a pas unicité d’isomorphismes. Eviter de dire « la ».  
 est une clôture algébrique de . (théorème fondamental de l’algèbre)  
Il existe des corps algébriquement clos dénombrables inclus dans , qui contiennent (strictement) le corps des nombres algébriques ; ce sont les clôtures algébriques des extensions transcendantes du corps des rationnels, comme celle de l’extension .  
**Théorème de Steinitz.** Tout corps possède une clôture algébrique. (par Zorn ou Krull (requiert AC))  
Deux clôtures algébriques de sont toujours reliées par un isomorphisme de corps laissant invariants les éléments de .  
Un polynôme irréductible de est dit **séparable sur**  ssi dans son corps de décomposition sur , il n’a pas de racine multiple / toutes ses racines sont simples. Dans le cas contraire il est dit **inséparable sur .**  
Par exemple, est irréductible et inséparable sur le corps de fractions .  
Sur un corps de caracteristique nulle, tout polynôme irréductible de est séparable sur K.  
Sur un corps de caracteristique un premier , un polynôme irréductible de est inséparable ssi .  
Un polynôme de réductible, dont tous les facteurs irréductibles sont séparables, est séparable.  
Un élément d’une extension algébrique est dit **séparable** ssi son polynôme minimal sur est séparable ssi n’est pas racine du polynôme minimal dérivé :   
Une **extension algébrique séparable**, est une extension algébrique dont tous les sont séparables.  
Un polynôme est séparable si et seulement s’il est premier avec sa dérivée formelle.  
Un polynôme irréductible est séparable si et seulement si sa dérivée formelle n’est pas nulle.  
Supposons *K* de caractéristique *p* et *P*(*X*) un polynôme irréductible. Il est séparable si et seulement s’il n’existe pas de polynôme *Q*(*X*) dans *K*[*X*] tel que l’on ait l’égalité .  
Soient *L* une extension algébrique de *K* et *M* une extension algébrique de *L*. Alors *M* est séparable sur *K* si et seulement si *M* est séparable sur *L* et *L* est séparable sur *K*.   
Un corps est dit **parfait** si toutes ses extensions algébriques sont séparables, autrement dit ssi tout polynôme irréductible de *K*[*X*] est séparable.   
Tout corps de caractéristique nulle est parfait.   
Un corps est parfait si et seulement s’il est de caractéristique nulle ou, lorsqu’il est de caractéristique , si l’endomorphisme de Frobenius est surjectif (autrement dit tout élément de *K* possède une racine *p*-ième dans ). En particulier tout corps fini est parfait.  
Tout corps algébrique sur un corps parfait est lui-même un corps parfait.  
En revanche, en caractéristique non nulle *p* (un nombre premier), tous les corps ne sont pas parfaits. Considérons le corps des fractions rationnelles sur le corps fini de cardinal *p*, *K* le sous-corps , et le polynôme irréductible de *K*[*Y*]. Alors l’élément *X* de *L* est racine multiple (d’ordre *p*) de *P*(*Y*), qui n’est donc pas séparable.  
Soit une extension finie de degré et une extension quelconque. Alors, il existe au plus -morphismes distincts . En fait, si M est algébriquement clos, alors est séparable ssi il existe exactement -morphisme distincts .  
**Théorème de l’élément primitif.** Tout extension finie séparable, est simple, c’est-à-dire engendrée par un seul élément appelé **l’élément primitif**.  
Une **extension normale de corps** est une extension algébrique de corps qui reste stable par tout morphisme d’extension vers une sur-extension de   
Autrement dit c’est une extension algébrique telle que tout polynôme irréductible de qui admet une racine sur , est scindé sur .  
Une extension de corps est normale et finie ssi cette extension est le corps de décomposition d’un polynôme non nul de .  
Les corps de décomposition sont les extensions normales finies.  
Les corps de rupture sont les extensions algébriques simples. **III. Utilisation de la théorie des groupes  
III.1. Automorphismes de corps – Groupe de Galois**Le **groupe de Galois d’une extension de corps ,**  est l’ensemble des -automorphismes d'extension de . Le groupe de Galois d’une extension de corps est un groupe.  
Le **groupe de Galois d’un polynôme non nul**  est le groupe de Galois du corps de décomposition du polynôme sur (donc vu comme une extension de ).  
**Th.** Soit un polynôme non nul sur un corps , de corps de décomposition , avec l’ensemble des racines de sur , alors tout -automorphisme de induit une bijection de sur , et est meme déterminé par cette permutation qu’il induit sur . Autrement dit, l’application qui a un -automorphisme de L, associe la permutation des indices induite sur , est un morphisme injectif de groupes. On retrouve le théorème de Cayley applique à ce groupe.  
On a , si est séparable, , si inseparable,   
Si est un produit d’irréductibles distincts , le théorème précèdent peut être précisé. En effet les définissent une bijection des racines de chacun des , il peut être donc préférable de voir comme un sous-groupe de avec nb de racines de .  
Pour 2 extensions de corps successives on a .   
Pour un sous-groupe d’un groupe de Galois , on définit **la sous-extension de invariante par**  :   
 est bien une sous-extension de , cad . Et   
Pour une extension , toute sous extension (on a ) vérifie :  
Exemples de calculs de groupe de Galois TODO (illisibles).  
Une **extension de Galois** est une extension (algébrique) normale et séparable. Autrement dit une extension algébrique dans laquelle le polynôme minimal de tout élément est scindé (vérifier).  
Le corps de décomposition du polynôme sur un corps de caracteristique est une extension normale, finie, et séparable, càd une extension galoisienne finie.  
De plus soit est un carré dans , et dans ce cas , ,   
soit n’est pas un carré dans , et dans ce cas   
**Th. de Galois, 1831.** Une extension algébrique finie est galoisienne ssi son degré est égal à l’ordre de son groupe de Galois . Dans ce cas pour galoisienne finie, la sous-extension invariante par le groupe de Galois n’est autre que le corps . Autrement dit   
**Théorème de Galois.** Soit une extension finie de Galois et son groupe de Galois. Alors les applications et établissent une bijection décroissante entre les extensions intermédiaires et les sous-groupes de .  
De plus, avec ces notations, une extension intermédiaire est de Galois ssi existe et dans ce cas .  
Exemple : Le groupe de Galois du polynôme sur est le groupe symétrique . Son corps de décomposition sur est de degré .  
Soit irréductible de degré premier impair (), ayant 2 racines complexes non réelles et racines réelles. Alors le groupe de Galois de sur correspond au groupe symétrique , et le corps de décomposition de est de degré dans . **III.2. Résolution par radicaux**Soient *K* un corps et *L* une extension de *K*.  
Un élément de *L* est dit **radical** sur *K* si l’une de ses puissances appartient à *K*.  
On dit qu’un élément de *L* s**’exprime par radicaux** sur *K* s’il est le dernier terme d’une suite finie de premier terme nul et dont chaque terme est radical sur l’extension de *K* engendrée par les termes précédents. Justification vague : créer des extensions sert à imbriquer des radicaux en créant des racines de polynômes.  
On dit que l’extension *L* de *K* est **résoluble par radicaux** si chaque élément de *L* s’exprime par radicaux sur *K*. Lorsque l’extension est finie, cela revient à dire que *L* est contenu dans une extension telle que tel que appartient à   
On dit qu’un polynôme est résoluble ou résoluble par radicaux si toutes ses racines s’expriment par radicaux sur *K*. Autrement dit : l’extension de *K* engendrée par les racines du polynôme est résoluble par radicaux.  
Si par exemple on a un polynôme de degré 3, on notera son groupe de Galois, son corps de décomposition, on cherche avec abéliens, ce qui donne une suite d’extensions intermédiaires ce qui facilite l’étude de . **III.2.1. Le cas du degré 3  
Th. Cardan.** TODO **III.2.2. Le cas du degré 4  
Th. Ferrari.** TODO **III.2.3. Le cas du degré   
Un groupe fini résoluble** est un groupe fini tel qu’il existe une suite finie de sous-groupes de verifiant et les groupes sont abéliens.  
Soit un polynôme de degré n, on note son corps de décomposition, corps de caracteristique nulle contenant les -iemes racines de l’unité pour tout . Alors est une **équation résoluble par radicaux** ssi il existe une suite finie d’extensions intermédiaires telles que l’extension est normale et est isomorphe a pour un certain degre et un certain .  
Le groupe n’est pas résoluble pour . **IV. Clôture algébrique de Q**On note l’ensemble des nombres complexes algébriques sur Q. est une extension de corps de degré infini. Le corps est une clôture algébrique de . est dénombrable.  
L’ensemble des nombres complexes transcendants sur est infini non dénombrable. ()

**Complément. Correspondance de Galois**démonstrations plus détaillées de la théorie de Galois

**Chapitre 13. Corps finis  
I. Clôture algébrique de**Pour premier, le corps admet une clôture algébrique . Cette clôture algébrique est dénombrable. Attention ici on ne définit que pour premier, la définition de sera différente.  
On note les polynômes irréductibles de (il en existe une infinité dénombrable).  
Si on note le corps de décomposition de sur , on a   
Une clôture algébrique d’un corps fini d’ordre premier *p* est un corps dénombrable. Pour tout entier naturel *n* non nul, il contient un et un seul sous-corps d’ordre , et il est égal à la réunion de tous ces sous-corps (ou plus savamment : leur limite inductive, avec avec *d* un diviseur de *n*). **II. Existence et unicité du corps à elements   
II.1. Unicité à isomorphisme près du corps à éléments**Un corps fini de caractéristique, un premier , de degré , possède éléments et  
 est le corps de décomposition du polynôme sur , tout corps a éléments est isomorphe à et l’extension est galoisienne finie, de degré n. **II.2. Existence du corps a éléments**Soit premier, et . L’ensemble des racines de est un corps a éléments isomorphe au corps de décomposition de sur . C’est un sous-corps de   
En résumé, il existe toujours un corps à éléments unique à isomorphisme près, c’est . **II.3. Groupe multiplicatif du corps a éléments**Rappel : L’exposant d’un groupe fini est le ppcm des ordres de ses éléments.  
Rappel : Tout groupe abélien fini est isomorphe a un et donc   
Sur un corps, pour , l’équation admet au plus solutions.  
Un groupe fini qui vérifie pour tout (divisant ) admet au plus solutions, est cyclique.  
Le groupe multiplicatif des inversibles du corps fini est cyclique.   
Tout groupe abélien fini admet un élément d’ordre l’exposant du groupe.  
Bien qu’identiques pour , le corps et l’anneau ne sont jamais isomorphes pour . **III. Sous-corps de   
III.1. Sous-corps et extensions**On a ssi divise et dans ce cas l’extension est galoisienne finie. **III.2. Automorphismes des corps finis**On appelle **automorphisme de Frobenius sur**  l’application .  
L’automorphisme de Frobenius sur est un automorphisme d’extension sur   
Le groupe de Galois de l’extension est cyclique d’ordre et engendré par l’automorphisme de Frobenius sur .   
La sous-extension de invariante par son groupe de Galois est le corps .  
   
 est aussi l’ensemble des éléments de laisses fixes par ou par le groupe engendre par , puisque les elements de sont les tels que . Le théorème de Galois prouve que les seuls automorphismes sont les puissances de l’automorphisme de Frobenius sur .  
Soit un diviseur de positif.  
 est cyclique d’ordre engendre par , c’est un sous-groupe de .  
   
Sur le diagramme suivant, represente un isomorphisme, les à gauche représentent un morphisme injectif, les à droite représentent un morphisme surjectif.  
  **III.3. Nouvelle construction de la clôture algébrique de**Pour tout admet une unique extension de degré : . Ce fait permet de simplifier la construction de .  
 **IV.1. Existence d’un polynôme irréductible de degré dans**Tout contient au moins un qui n’appartient à aucun avec diviseur strict de . Autrement dit la réunion des sous-corps de est strictement incluse dans .  
Pour un tel alors est un polynôme de , irréductible, séparable, et de degré . De plus le corps de rupture de sur est aussi le corps de décomposition de ce polynôme. Le morphisme de -algèbres est un isomorphisme. **IV.2. Corps finis via la caractéristique nulle.**On a vu que pour tout premier et entier a au moins un polynôme irréductible de degré n, soit , et soit le polynôme correspondant dans . est irréductible dans   
Alors est un corps fini a éléments donc isomorphe a   
De plus est un idéal maximal de .  
Attention un idéal de la forme avec premier et irréductible n’est pas forcément un idéal maximal : contre-exemple fournit par  **IV.3. Dénombrement des polynômes irréductibles**Pour tout le polynôme est exactement le produit de tous les polynômes unitaires irréductibles de dont le degré divise .  
En notant le **nombre de polynômes unitaires irréductibles de degré dans**  on a   
Ces égalités pour permettent de calculer successivement les nombres   
Par exemple on calcule avec les égalités  **IV.4. Exemples de corps finis**Pour effectuer des calculs dans il faut pouvoir nommer ses éléments, puis les additionner et les multiplier. La construction du corps de rupture d’un polynôme indique la démarche à suivre : trouver un polynôme unitaire irreductible de degre dans , utiliser l’isomorphisme et effectuer les calculs dans . Cependant en général, pas de méthode canonique pour trouver parmi les possibles. De plus . Parmi les polynômes unitaires environ est irréductible.  
Exemple de TODO **V. Polygones réguliers constructibles à la règle et au compas  
Gauss, 1796\*.** Le polygone régulier à 17 côtés est constructible à la règle et au compas.   
**Gauss, 1796\*.** Le polygone régulier à côtés est constructible à la règle et au compas ssi ou et sont des nombres premiers distincts de la forme c’est-à-dire des nombres de Fermat.  
Lemmes :  
Le polynôme minimal sur d’une racine primitive -ieme de l’unité avec premier est le -ieme polynome cyclotomique (preuve par critère Eisenstein)  
Le polynôme minimal sur d’une racine primitive -ieme de l’unité avec premier est le -ieme polynome cyclotomique   
Le polygone régulier à côtés avec premier impair, n’est pas constructible à la règle et au compas. **VI. Théorème de Wedderburn**  
Tout corps au sens large (commutatif ou non) fini est automatiquement commutatif.  
Tout anneau intègre fini est un corps.  
**Complément : Quaternions  
1. Construction des quaternions  
L’ensemble des quaternions**  est un Rev de dimension et un corps non commutatif appelé algèbre des quaternions.  
Le groupe spécial unitaire est un sous-groupe multiplicatif de et ssi   
On pose qui forme une base de   
   
 Tout quaternion non nul est inversible d’inverse avec   
On peut définir l’isomorphisme d’ev   
L’image de la base est donc une b.o.n qu’on supposera directe.  
Via cet isomorphisme, les opérations de s’écrivent : et   
L’algèbre des quaternions possède une infinité de racines de .  
Le **conjugue d’un quaternion** est .  
On a   
La **norme d’un quaternion**  est elle est bien définie car . Elle coincide avec la norme euclidienne sur .  
On a   
L’inverse d’un quaternion non nul est   
On a et   
  **2. Paramétrage de et de via les quaternions**L’isomorphisme fournit une bijection entre et la sphère unité de   
En munissant et de leur structure naturelle d’espace topologique (fermés de ), cette bijection est un homéomorphisme. Par transport de structure, est un groupe. est simplement connexe, il en est donc de même pour . Autrement dit tout chemin fermé sur est homotope a un point.  
Un **quaternion réel** est un quaternion de la forme avec   
Un **quaternion pur** est un quaternion de la forme avec   
Identifions avec l’espace vectoriel de des quaternions purs.  
Soit un quaternion de norme 1  
On peut écrire avec quaternion pur de norme associe a un vecteur unitaire   
L’application est la rotation d’angle autour de . L’application est un morphisme de groupes continu et surjectif de noyau , autrement dit on a la suite exacte   
Pour ou , soit la rotation d’angle autour du vecteur unitaire . Alors la rotation composée est la rotation définie par le quaternion   
   
TODO