

Cours 1

Un peu d'histoire de l'algèbre: Babylone, Euclide, Bramagupta, Al' Jabr de Al-Khwarizmi, Cardan, Gauss, Emmy Noether, Emil Artin, Alexandre Grothendieck.

Théorème de d'Alembert (fundamental theorem of algebra): C est algébriquement clos (sans démonstration).

Un corps fini $\mathbf{F}_q$ n'est pas algébriquement clos.

Euclide: Il y a une infinité de nombres premiers.

Tout corps fini est d'ordre une puissance d'un nombre premier p .

$\mathbf{Z}/p\mathbf{Z}$ est un corps.

Anneaux commutatifs unitaires, intègres, diviseurs de 0, idéaux, idéal principal.

Anneau principal : intègre et tout idéal est principal.

$\mathbf{Z}$ est principal, $K[X]$ est principal si K est un corps (commutatif).

Somme de deux idéaux.

Un idéal I de l'anneau A est maximal si et seulement si l'anneau quotient est un corps.

L'inclusion $Aa \subset Ab$ est équivalente à b divise a (il existe $c \in A$ tel que $a = bc$).

$p\mathbf{Z}$ est un idéal maximal de $\mathbf{Z}$ par le théorème de factorisation en produit de nombres premiers.

Morphismes d'anneaux, morphismes fondamentaux $A \rightarrow A/I$, $\mathbf{Z} \rightarrow A$.

Caractéristique d'un anneau. La caractéristique d'un anneau intègre est 0 ou un nombre premier.

Un corps fini est un espace vectoriel de dimension finie sur $\mathbf{Z}/p\mathbf{Z}$ pour un nombre premier.

Factorisation d'un morphisme $A \rightarrow B$ par un morphisme surjectif $A \rightarrow A/I$.

Cours 2

Si K est un corps, l'anneau $K[X]/PK[X]$ est un corps si et seulement si P est irréductible

Élément irréductible dans un anneau commutatif A (pas une unité, de diviseurs triviaux modulo les unités)

Un élément a de A est une unité si et seulement si $Aa = A$.

Soit A un anneau intègre. Un élément a de A est irréductible si et seulement si Aa est un idéal maximal parmi les idéaux principaux de A .

Le groupe des unités $K[X]^*$ est égal à $K^* = K - 0$ par le lemme du degré.

Un anneau intègre fini est un corps.

Soit $a \in A$. Le morphisme d'anneau "évaluation en a " induit un isomorphisme $A[X]/(X-a)A[X] \simeq A$.

Soit $a \in A, P \in A[X]$. Alors $P(a) = 0$ est équivalent à $X - a$ divise P .

$X^n - a^n = (X - a)(X^{n-1} + aX^{n-2} + \dots + a^{n-1})$ pour tout entier $n \geq 1, a \in A$.

Un morphisme bijectif d'anneau $f : A \rightarrow B$ est un isomorphisme.

Théorème (Classification des corps finis). Pour tout nombre premier p et tout entier $f \geq 1$, il existe un unique corps fini ayant $q = p^f$ éléments, à isomorphisme près. Sans démonstration.

Un corps F à p éléments est isomorphe à $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ (via le morphisme fondamental $\mathbf{Z} \rightarrow F$)

Si F est un corps à q éléments, alors F contient $\mathbf{F}_p$ et $X^q - X = \prod_{a \in F} (X - a)$. C'est le "corps des racines du polynôme $X^q - X$ sur $\mathbf{F}_p$."

Théorème (Construction d'extensions $F \subset K$). Soit F un corps et $P \in F[X]$ un polynôme irréductible de degré $f \geq 1$. Alors

- le morphisme canonique $F[X] \rightarrow F[X]/PF[X]$ restreint à F est injectif (par le lemme du degré),
- le corps $K = F[X]/PF[X]$ vu comme un espace vectoriel sur F a une dimension finie égale au degré de P (par la division euclidienne).

Cours 3

Théorème. Pour tout nombre premier p , pour tout entier $n \geq 1$, il existe un polynôme irréductible $P \in \mathbf{F}_p[X]$ de degré n (sans démonstration).

Application à l'existence de corps finis ayant p^n éléments.

Exemple: Corps finis ayant ≤ 16 éléments.

$X^2 + X + 1 \in \mathbf{F}_2[X]$ est l'unique polynôme irréductible unitaire de degré 2,

$P = X^3 + X + 1, X^3 + X^2 + 1 \in \mathbf{F}_2[X]$ sont irréductibles, les corps finis $\mathbf{F}_2[X]/(P)$ ayant 8 éléments sont isomorphes, par l'isomorphisme canonique déduit de $X \rightarrow X + 1$.

Si F est un corps, un polynôme de degré ≤ 3 dans $F[X]$ est irréductible si et seulement s'il n'a pas de racines dans F

$X^4 + X + 1, X^4 + X^3 + 1 \in \mathbf{F}_2[X]$ sont irréductibles, car $X^4 + X^2 + 1$ est le seul polynôme réductible sans racines dans $\mathbf{F}_2$.

$(a+b)^p = a^p + b^p$ pour deux éléments a, b d'un anneau de caractéristique p .

Morphisme de Frobenius $a \mapsto a^p$ dans un anneau de caractéristique p .

$\mathbf{Z}[X]$ n'est pas un anneau principal.

Lemme du degré dans $A[X]$: Si $P, Q \in A[X]$ alors $\deg(PQ) \leq \deg(P) + \deg(Q)$ avec égalité si le coefficient dominant de P ne divise pas 0.

division euclidienne dans $A[X]$: Si $P, Q \in A[X]$ et le coefficient dominant de $P \neq 0$ est inversible, il existe des polynômes uniques $R, S \in A[X]$ vérifiant $Q = PS + R$, $R = 0$ ou $\deg(R) < \deg(P)$.

Si $A \subset B$ est une inclusion d'anneaux, $P, Q \in A[X]$ et P unitaire de degré ≥ 1 . Si P divise Q dans $B[X]$ alors P divise Q dans $A[X]$.

Module M sur un anneau, base (finie) d'un module libre.

Si $P \in A[X]$ est unitaire, alors $A[X]/PA[X]$ est un A -module libre de rang $\deg P$.

$\mathbf{Z}/6\mathbf{Z} \simeq \mathbf{F}_2 \times \mathbf{F}_3$.

Produit de deux idéaux dans un anneau A , deux idéaux I, J sont premiers entre eux si $I + J = A$.

$ICapJ = IJ$ si $I + J = A$.

Lemme chinois. Si I, J sont deux idéaux premiers entre eux dans un anneau A , alors A/IJ est isomorphe à $A/I \times A/J$.

n est entier ≥ 0 , alors $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/p_1^{k_1}\mathbf{Z} \times \dots \times \mathbf{Z}/p_r^{k_r}\mathbf{Z}$ si $n = p_1^{k_1} \dots p_r^{k_r}$, $p_i \neq p_j$ premiers pour $1 \leq i \neq j \leq r$ and $k_i \geq 1$.

F est un corps, $P \in F[X]$ unitaire de degré ≥ 1 , alors $F[X]/PF[X] \simeq F[X]/P_1^{k_1}F[X] \times \dots \times F[X]/P_r^{k_r}F[X]$ si $P = P_1^{k_1} \dots P_r^{k_r}$, $P_i \neq P_j$ irréductibles unitaires pour $1 \leq i \neq j \leq r$ and $k_i \geq 1$.

Cours 4

Un anneau A est factoriel s'il est intègre et si tout élément $a \neq 0$ admet une factorisation unique: $a = u \prod_{p \in P} p^{v_p(x)}$ où P est un système de représentants des irréductibles modulo multiplication par les unités, $u \in A^*$, $v_p(x) \in \mathbf{N}$ égal à 0 sauf pour un nombre fini de p , $u, v_p(x)$ uniques.

dans un anneau factoriel A , pour $a, b \in A$, on a $v_\gamma(ab) = v_\gamma(a) + v_\gamma(b)$ pour tout $\gamma \in P$.

dans un anneau factoriel, il existe un p.g.c.d. et un p.p.c.m. définis modulo multiplication par les unités.

$v_\gamma(p.g.c.d.(a, b)) = \min(v_\gamma(a), v_\gamma(b))$, $v_\gamma(p.p.c.m.(a, b)) = \sup(v_\gamma(a), v_\gamma(b))$.

Un idéal I d'un anneau A est premier si A/I est intègre, i.e. pour $a, b \in A$, alors $ab \in I$ implique a ou b appartient à I .

Idéal maximal implique idéal premier.

Théorème: A principal implique A factoriel implique $A[X]$ factoriel.

Si A est intègre, alors $A[X]$ est intègre et $A[X]^* = A^*$ (lemme du degré)

A factoriel est équivalent à: A intègre et

1) Si $p \in A$ est irréductible, alors l'idéal Ap est premier (unicité de la factorisation)

2) Toute suite croissante d'idéaux principaux de A est stationnaire (existence de la factorisation).

Cours 5

Un nombre entier $n \in \mathbf{Z}$ est irréductible si et seulement s'il est irréductible dans $\mathbf{Z}[X]$ (lemme du degré).
Même résultat pour un anneau A intègre.

Un polynôme $P \in \mathbf{Z}[X]$ est dit primitif s'il est de degré ≥ 1 et si le p.g.c.d. de ses coefficients est ± 1 .
Même définition pour un anneau factoriel en remplaçant ± 1 par A^* .

$\mathbf{Z}[X] \rightarrow \mathbf{F}_p[X]$ Réduction modulo p

Morphisme d'anneau canonique $A[X] \rightarrow B[X]$ associé à un morphisme d'anneau $f: A \rightarrow B$

Le produit de deux polynômes primitifs est primitif.

Un polynôme $P \in \mathbf{Z}[X]$ primitif, de coefficient dominant non divisible par p , irréductible dans $\mathbf{F}_p[X]$ est irréductible dans $\mathbf{Z}[X]$.

$X^4 + 1728X^3 + 9572X^2 + 551X + 3577$ est irréductible dans $\mathbf{Z}[X]$.

Critère d'Eisenstein: Un polynôme $P \in \mathbf{Z}[X]$ unitaire, dont les coefficients non dominants sont divisibles par p , et le coefficient constant n'est pas divisible par p^2 est irréductible dans $\mathbf{Z}[X]$.

$X^{657} - 32X^{67} + 4X - 2$ est irréductible dans $\mathbf{Z}[X]$.

Contenu d'un polynôme $P \in \mathbf{Q}[X]$ de degré ≥ 1 : un élément $c(P) \in \mathbf{Q}$ tel que $P = c(P)P_1$ où P est un polynôme primitif dans $\mathbf{Z}[X]$. Unique modulo ± 1 .

$c(PQ) = \pm c(P)c(Q)$ pour deux polynômes $P, Q \in \mathbf{Q}[X]$ de degré ≥ 1 .

$P \in \mathbf{Z}[X]$ si et seulement si $c(P) \in \mathbf{Z}$, est primitif si et seulement si $c(P) = \pm 1$

Un polynôme $P \in \mathbf{Z}[X]$ primitif est irréductible dans $\mathbf{Z}[X]$ si et seulement s'il est irréductible dans $\mathbf{Q}[X]$.

$\mathbf{Z}[X]$ est un anneau factoriel (factoriser $c(P)$ dans $\mathbf{Z}$ et P_1 dans $\mathbf{Q}[X]$).

Cours 6

A intègre, I idéal premier : $P \in A[X]$ irréductible dans $A/I[X]$ de coefficient dominant n'appartenant pas à I , est irréductible dans $A[X]$.

A anneau factoriel.

- Critère d'Eisenstein: $p \in A$ irréductible, $P \in A[X]$ primitif, de coefficient dominant non divisible par p , autres coefficients sont divisibles par p , terme constant on divisible par p^2 , est irréductible.

- Le produit de deux polynômes primitifs est primitif est vrai (donc ses conséquences: l'unicité du contenu d'un polynôme de $\text{Frac}A[X]$ modulo A^* , la formule du produit du contenu, un polynôme primitif est irréductible dans $A[X]$ si et seulement s'il est irréductible dans $\text{Frac}A[X]$, $A[X]$ est factoriel.

Si un anneau A est contenu dans un corps K . Alors $\{ab^{-1}, a \in A, b \in A - 0\}$ est un sous-corps F_K de K . C'est le plus petit corps contenant A .

Un morphisme injectif d'anneau $A \rightarrow E$ dans un corps E se prolonge uniquement à F_K , induit un isomorphisme $F_K \simeq F_E$.

Si A est intègre, $A \times (A - 0)$ modulo la relation d'équivalence $a/b \equiv c/d$ si $ad = bc$ est un corps qui contient A .

Théorème: Un anneau intègre A est contenu dans un corps, le "plus petit" s'appelle le corps des fractions $\text{Frac}A$ de A , unique à isomorphisme près.

Un morphisme de corps est nul ou injectif.

Localisation AS^{-1} d'un anneau intègre A par un système multiplicatif S .

$\mathbf{Z}[1/2] = \mathbf{Z}(1/2^{\mathbf{N}})^{-1}$

L'ensemble des entiers non divisibles par un nombre premier p est un système multiplicatif $S(p)$, $\mathbf{Z}S(p)^{-1}$. Unique idéal maximal $p\mathbf{Z}S(p)^{-1}$.

A anneau intègre, I idéal premier, $S(I) = A - I$ système multiplicatif, $AS(I)^{-1}$ a un unique idéal maximal $IAS(I)^{-1}$.

Zorn: Un ensemble ordonné E tel que toute partie totalement ordonnée possède un majorant dans E , admet un élément maximal

Tout idéal $I \neq A$ d'un anneau A est contenu dans un idéal maximal.

$A^* = A - M$ pour un anneau A ayant un unique idéal maximal M .

Un nombre complexe z est algébrique s'il est racine $P(z) = 0$ d'un polynôme unitaire $P \in \mathbf{Q}[X]$ de degré ≥ 1 .

Théorème. L'ensemble des nombres algébriques est un corps algébriquement clos $\mathbf{Q}^a$.

définition-Proposition. Soit L/K est une extension de corps. Un élément $x \in L$ est algébrique sur K s'il vérifie les propriétés équivalentes

- x est racine $P(x) = 0$ d'un polynôme unitaire $P \in K[X]$ de degré ≥ 1 .

- $K[x]$ est un corps.

- $K[x]$ est un espace vectoriel de dimension finie sur K .

- Le noyau du K -morphisme canonique $K[X] \rightarrow K[x] \subset L$ est non nul.

Le polynôme unitaire $P \in K[X]$ de plus petit degré tel que $P(x) = 0$ (générateur du noyau) est irréductible, s'appelle le polynôme irréductible de x sur K .

Un K -sous espace vectoriel d'un K -espace vectoriel de dimension finie est de dimension finie.

La somme et le produit de $x, y \in L$ algébriques sur K est algébrique sur K . L'inverse de x est algébrique sur K si $x \neq 0$.

Cours 7

Base télescopique.

Extension finie E/K : le K -espace vectoriel E est de dimension finie $[E : K]$ sur K .

Extension algébrique E/K : tout élément de E est algébrique sur K .

Un élément algébrique sur E est algébrique sur K , si E/K est algébrique.

déviage. Si $K \subset E \subset L$, alors L/K est finie (algébrique) si et seulement $E/K, L/E$ sont finies (algébriques); alors $[L : K] = [L : E][E : K]$.

$\mathbf{Q}^a$ est le “plus petit” corps algébriquement clos contenant $\mathbf{Q}$.

$\mathbf{Q}[X]$ est dénombrable (“dénombrable” est stable par union, produit fini).

$\mathbf{Q}^a$ est dénombrable, alors que le cardinal de $\mathbf{C}$ est la puissance du continu.

Proposition (sans démonstration). Le cardinal d’une extension algébrique E d’un corps infini K est égal au cardinal de K .

Théorème: 1) Un corps K est contenu dans un corps algébriquement clos E .

2) L’ensemble des éléments de E algébriques sur K est une extension algébrique de K , algébriquement close, appelé la clôture algébrique K^a de K dans E . Toute extension de K contenue dans E contient K^a . (Même démonstration que pour $K = \mathbf{Q}$).

3) deux clôtures algébriques de K sont isomorphes.

Soit $P \in K[X]$ irréductible, alors P a une racine dans le corps $K[X]/PK[X]$ (la classe x de X).

dans l’anneau de polynômes $A = K[X_P]$, pour tout $P \in K[X] - K$ à plein de variables, l’idéal I engendré par $P(X_P)$ pour tout $P \in K[X] - K$ ne contient pas 1 (Si 1 est une somme finie $\sum g_i P_i(X_{P_i})$, choisir une extension F/K où les P_i ont une racine α_i puis spécialiser $X_{P_i} \rightarrow \alpha_i$, on obtient $1 = 0$). Si M est un idéal maximal de A contenant I , tout polynôme $P \in K[X]$ a une racine dans le corps A/M .

Si $K = E_0 \subset E_1 \subset \dots \subset E_n \subset \dots$ est une suite de corps tels que tout polynôme $P \in E_n[X]$ a une racine dans E_{n+1} , pour tout $n \geq 0$, alors $E = \bigcup_n E_n$ est un corps algébriquement clos (si $P \in E[X]$, il existe $n \geq 1$ tel que $P \in E_n[X]$) contenant K .

dérivée P' d’un polynôme $P \in A[X]$. Formule du produit $(PQ)' = PQ' + P'Q$.

Soit $a \in A$. Si $P \in A[X]$ est divisible par $(X - a)^2$ si et seulement P et P' sont divisibles par $X - a$.

Pour tout nombre premier p et pour tout entier $n \geq 1$, l’ensemble des racines de $X^{p^n} - X$ dans $\mathbf{F}_p^a$ est un corps $\mathbf{F}_{p^n}$ à p^n éléments, c’est l’unique corps à p^n éléments contenu dans $\mathbf{F}_p^a$.

Cours 8 Soient d, n deux entiers ≥ 1 . Alors $d|n$ est équivalent à $\mathbf{F}_{p^d} \subset \mathbf{F}_{p^n}$, est équivalent à $X^{p^d-1} - 1$ divise $X^{p^n-1} - 1$, est équivalent à $a^d - 1$ divise $a^n - 1$ pour un entier $a > 1$, est équivalent à $a^d - 1$ divise $a^n - 1$ pour tout entier $a > 1$.

Soit $P \in K[X]$ irréductible, et L/K une extension de corps. Un K -morphisme $K[X]/PK[X] \rightarrow L$ est déterminé par l’image de x = classe de X modulo $PK[X]$, qui est une racine quelconque de $P(X)$ dans L .

Soit $x \in K^a$ et P le polynôme minimal de x sur K . Alors le nombre de K -morphisms $K[x] \rightarrow K^a$ est égal au degré de P , si les racines de P sont simples.

Soit N_n le nombre de polynômes irréductibles unitaires de degré n dans $\mathbf{F}_p[X]$.

Exemple $N_1 = p, N_2 = (p^2 - p)/2$.

Alors $p^n = \sum_{d|n} dN_d$.

La fonction de Moebius $\mu(1) = 1, \mu(p_1 \dots p_r) = (-1)^r, \mu(p^2 n) = 0$ pour tous nombres premiers distincts $p_1, \dots, p_r$ et p nombre premier, n entier ≥ 1 .

Formule d’inversion de Moebius $nN_n = \sum_{d|n} \mu(n/d)p^d$ (sans démonstration)

Application: $p^n \neq \sum_{1 \leq r < n} up^r$ avec $u \in \{0, \pm 1\}$ donc $N_n \neq 0$.

Cours 9

$(p^n - p^{[n/2]+1}) \leq nN_n \leq p^n$ car $\sum_{d|n, d \neq n} dN_d \leq 1 + p + \dots + p^{[n/2]}$.

Application $N_n \neq 0$ for $n \geq 3$.

$\mathbf{F}_{p^n} \simeq \mathbf{F}_p[X]/P[X]$ pour tout $P \in \mathbf{F}_p[X]$ irréductible unitaire de degré n .

Un polynôme irréductible $P \in \mathbf{F}_p[X]$ a ses racines simples (divise $X^{p^n} - X$) et contenues dans $\mathbf{F}_{p^n}$.

Si $x \in \mathbf{F}_p^a$ est une racine de $P \in \mathbf{F}_p[X]$ irréductible unitaire de degré n , alors $\mathbf{F}_{p^n} = \mathbf{F}_p[x]$. On dit que x est un élément primitif de $\mathbf{F}_{p^n}$.

$\mathbf{F}_{p^n}^*$ est cyclique, engendré par x (utiliser que l’ordre d’un élément divise $p^n - 1$ donc est $p^d - 1$ pour $d|n$).

Le Frobenius $x \rightarrow x^p$ est un automorphisme de $\mathbf{F}_{p^n}$ d'ordre n .

Le groupe des automorphismes de $\mathbf{F}_{p^n}$ est cyclique engendré par le Frobenius

Un sous-groupe fini G du groupe multiplicatif d'un corps commutatif fini est cyclique. Se ramener au cas d'un groupe d'ordre p^k , avec p premier, $k \geq 1$, prendre l'élément de G d'ordre maximal p^r , puis utiliser que tout élément de G est racine de $X^{p^r} - 1$, qui a au plus p^r racines dans un corps commutatif.

Factorisation d'un groupe fini commutatif en p -groupes. Si G est d'ordre $n = p_1^{k_1} \dots p_r^{k_r}$ est la factorisation en produit de nombres premiers distincts $p_i \neq p_j$ si $i \neq j$, d'exposants $k_i \geq 1$, alors $G = G(p_1^{k_1}) \times \dots \times G(p_r^{k_r})$ où les $G(p_i^{k_i})$ sont des p_i -groupes (d'ordre une puissance de p_i , nécessairement $p_i^{k_i}$).

Un groupe commutatif = un $\mathbf{Z}$ -module.

Un K -espace vectoriel muni d'un endomorphisme = un $K[X]$ -module.

Somme directe de A -modules. Soit A un anneau commutatif, M_1, M_2 deux sous-modules d'un A -module M . Alors le morphisme naturel $M_1 \times M_2 \rightarrow M$ est surjectif si et seulement si $M = M_1 + M_2$, injectif si et seulement si $M_1 \cap M_2 = 0$. S'il est bijectif, on dit que $M = M_1 \oplus M_2$ est la somme directe de M_1 et de M_2 .

Si A est un anneau principal, M un A -module, $aM = 0$ annulé par $a \in A$ de factorisation $a = p_1^{k_1} \dots p_r^{k_r}$ est la factorisation en produit d'irréductibles distincts $p_i \neq p_j$ si $i \neq j$, d'exposants $k_i \geq 1$, alors M est une somme directe $M = M(p_1^{k_1}) \oplus \dots \oplus M(p_r^{k_r})$ de sous-modules $M(p_i^{k_i})$ annulé par $p_i^{k_i}$. Ecrire $a = p_1^{k_1} b$, par Bezout il existe $x, y \in A$ tel que $1 = xp_1^{k_1} + yb$, alors $bM = M(p_1^{k_1})$ est annulé par $p_1^{k_1}$ et $p_1^{k_1}M = M(b)$ est annulé par b . L'intersection est nulle. On continue avec b .

Polynôme cyclotomique $\Phi_n(X) = \prod_{(k,n)=1} (X - e^{2i\pi k/n})$, de degré l'indicateur d'Euler.

$\phi(n) = \phi(p_1^{k_1}) \times \dots \times \phi(p_r^{k_r})$, $\phi(p^k) = p^k - p^{k-1}$.

$\phi(n)$ pour $n \leq 12$.

Théorème. $\Phi_n(X) \in \mathbf{Z}[X]$ est irréductible.

Cours 10

Irréductibilité de Φ_n . Si $\Phi_n = PQ$ avec $P, Q \in \mathbf{Z}[X]$ de degré ≥ 1 , x une racine de l'unité d'ordre n telle que $P(x) = 0$, p nombre premier ne divisant pas n , alors $P(x^p) = 0$. Sinon $Q(x^p) = 0$. On a $x \in A := \mathbf{Z}[e^{2i\pi/n}]$. Soit M un idéal maximal de A contenant p . Dans A/M , on a $Q(x^p) = Q(x)^p$ donc $Q(x) = 0 = P(x)$. Or les racines de $X^n - 1$ dans A/M sont simples. Absurde. On en déduit que x^k pour tout entier k , $(k, n) = 1$, sont racines de P par induction sur le nombre de facteurs premiers de k .

C_n groupe cyclique d'ordre $n \geq 1$. Si x est un générateur, les autres générateurs sont $x^k, 1 \leq k \leq n, (k, n) = 1$. L'unique sous-groupe C_d d'ordre $d|n$ est engendré par $x^{n/d}$.

$q = p^f, f \geq 1$. Le groupe de Galois $\text{Aut}_{\mathbf{F}_q} \mathbf{F}_{q^n} \simeq C_n$ est engendré par $\phi : x \mapsto x^q$. Le corps $\mathbf{F}_{q^d}$ est le corps des invariants de $\mathbf{F}_{q^n}$ par $C_{n/d}$. Bijection entre sous-groupes du groupe de Galois et sous-extensions de $\mathbf{F}_{q^n}/\mathbf{F}_q$.

Entier algébrique: racine complexe d'un polynôme unitaire $P \in \mathbf{Z}[X]$.

Exemple: la longueur $\sqrt{2}$ de la diagonale du carré unité, le nombre d'or $(1 + \sqrt{5})/2$ racine positive de $X^2 - X - 1$.

Entiers quadratiques: d entier sans facteurs carré, l'anneau des entiers du corps quadratique $\mathbf{Q}[d^{1/2}]$, est $\mathbf{Z} \oplus \mathbf{Z}d^{1/2}$ si $d \equiv 2, 3 \pmod{4}$ et $\{(m + nd^{1/2})/2, m, n \in \mathbf{Z}, m \equiv n \pmod{2}\} = \mathbf{Z} \oplus \mathbf{Z}(1 - d^{1/2})/2$ si $d \equiv 1 \pmod{4}$. $x + yd^{1/2}$ entier pour $x, y \in \mathbf{Q}$ est équivalent à $2x, x^2 - dy^2$ entiers.

Trace, norme $\mathbf{Q}[d^{1/2}] \rightarrow \mathbf{Q}$.

Si x est un entier algébrique et f un automorphisme de $\mathbf{C}$, alors $f(x)$ est un entier algébrique.

Le groupe des automorphismes de $\mathbf{Q}[d^{1/2}]$ est d'ordre 2.

Théorème (démonstration plus loin). L'ensemble des entiers algébriques est un anneau $\mathbf{Z}^a$, l'anneau des entiers algébriques.

L'anneau des entiers d'un corps de nombres.

Généralisation: $A \subset B$ une inclusion d'anneaux, $b \in B$ est entier sur A s'il existe $P \in A[X]$ unitaire tel que $P(b) = 0$. La clôture intégrale de A dans B est l'ensemble des éléments de B entiers sur A . C'est un anneau.

Anneau intègralement clos: intègre, égal à sa clôture intégrale dans son corps des fractions.

L'anneau des entiers d'un corps de nombres est intègralement clos.

Un anneau factoriel est intègralement clos (si ab^{-1} entier avec a, b premiers entre eux, $a^n \in bA$).

Entiers cyclotomiques (sans démonstration): $\mathbf{Z}[e^{2i\pi/n}]$ est l'anneau des entiers du n -ième corps cyclotomique $\mathbf{Q}[e^{2i\pi/n}]$.

Le groupe des automorphismes de $\mathbf{Q}[e^{2i\pi/n}]$ est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$.

Cours 11

Théorème (sans démonstration) Le groupe $(\mathbf{Z}/2^k\mathbf{Z})^*$ est isomorphe à $(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2^{k-2}\mathbf{Z})$ si $k \geq 3$. Pour p premier impair ou pour $p = 2, k = 1, 2$, $(\mathbf{Z}/p^k\mathbf{Z})^*$ est cyclique (donc isomorphe à $\mathbf{Z}/p^{k-1}(p-1)\mathbf{Z}$).

Si $K \subset L$ est une extension de corps, et H un sous-groupe de $\text{Aut}_K L$, alors l'ensemble L^H des H -invariants de L est un corps.

Les propriétés suivantes sont équivalentes:

- 1) b est entier,
- 2) le A -module $A[b]$ est de type fini,
- 3) $A[b]$ est contenu dans un A -module de type fini M , $bM \subset M$, et pas d'élément $d \in A[b]$ non nul tel que $dM = 0$.

Application: Si b_1, b_2 entiers sur A , alors $A[b_1, b_2]$ est un A -module de type fini, donc tous ses éléments sont entiers, en particulier $b_1 + b_2, b_1 b_2$.

Preuve des équivalences. 1) entraîne 2) entraîne 3) (prendre $M = A[b]$) entraîne 1): Astuce du déterminant et cofacteurs.

Prendre $(m_i) \in M^n$ engendrant M , écrire $bm_i = \sum_j a_{ij}m_j$ puis $\sum_j (a_{ij} - b\delta_{ij})m_j = 0$. Multiplier par le cofacteur b_{ik} de la matrice $(a_{ij} - b\delta_{ij}) \in M(n, A[b])$ et prendre la somme sur i . Si d est le déterminant de la matrice on obtient $dm_k = 0$ pour tout k , donc $dM = 0$, donc $d = 0$. Or $d = P(b)$, $P \in A[X]$ de coefficient dominant ± 1 .

Cayley-Hamilton. $f \in \text{End}_A M$, il existe $P \in A[X]$ tel que $P(f) = 0$.

Forme multilinéaire alternée $f : M^n \rightarrow A$. Linéaire en chaque variable, nulle si deux coordonnées adjacentes sont égales $m_i = m_{i+1}$.

$f(\dots, m_i, m_{i+1}, \dots) = -f(\dots, m_{i+1}, m_i, \dots)$.

Hypothèse "adjacent" inutile.

Si $(v_i), (w_i) \in M^n$ et $w_j = \sum_i a_{ij}v_i$ pour $(a_{ij}) \in M(n, A)$, alors $f(w_i) = (\sum_{s \in S_n} (-1)^{\epsilon(s)} \prod a_{is(i)}) f(v_i)$.

Si $M \simeq A^n$ a une base (v_i) , alors f est déterminée par $f(v_i)$.

Déterminant d'une matrice $A = (a_{ij}) \in M(n, R)$ de matrice colonnes $C_i \in R^n$: $\det(a_{ij}) = f(C_i) = \sum_{s \in S_n} (-1)^{\epsilon(s)} \prod a_{is(i)}$ pour la forme multilinéaire alternée telle que $f(e_i) = \det(\text{Id}) = 1$, et (e_i) est la base canonique de R^n .

R anneau commutatif. $\det AB = (\det A)(\det B)$ pour deux matrices $A, B \in M(n, R)$ est égal au produit des déterminants. Appliquer $f(w_i) = (\det A)f_{v_i} = (\det A)(\det B)f_{e_i} = \det AB f(e_i)$ dans $M = R^n$ en prenant $v_i = \sum_j b_{ij}e_j$ et (e_i) la base canonique de R^n .

Matrice transposée $(b_{ij} = a_{ji}) \in M(n, A)$: même déterminant.

Développement du déterminant $d = \det(a_{ij})$ selon la ligne i

$d = (-1)^{i+1} a_{i1} \det B(i1) + (-1)^{i+2} a_{i2} \det B(i2) + \dots + (-1)^{i+n} a_{in} \det B(in)$

$B(ij) :=$ matrice (a_{ij}) privée de la ligne i et de la colonne j .

Cofacteur $b_{ij} := (-1)^{i+j} \det B(ij)$, matrice transposée des cofacteurs $(b_{ji}) \in M(n, A)$

Développement du déterminant $d = \det(a_{ij})$ selon la colonne j , que l'on remplace par C_k

$\sum_i a_{ij} b_{ik} = d \delta_{jk}$.

$(a_{ij}) \times (b_{ji}) = d I_n$, I_n matrice identité de $M(n, A)$.

Cours 12

Lemme de Nakayama. Soit M un A -module de type fini et I un idéal de A tel que $IM = M$. Alors il existe $a \in A$ tel que $aM = M$, et $a \in 1 + I$.

Soit M un A -module de type fini. Un morphisme $f : M \rightarrow M$ surjectif est injectif.

Les bases d'un A -module libre de type fini ont le même nombre d'éléments.

$(2, 3) =$ système de générateurs minimal du $\mathbf{Z}$ -module $\mathbf{Z}$.

Sous-module N d'un A -module M , noyau d'une application linéaire $f : M \rightarrow M'$, module quotient $p : M \rightarrow M/N$.

Morphismes canoniques: f induit un morphisme injectif $M_1/\text{Ker } f \rightarrow M'$, d'image $f(M)$.

$N \rightarrow N + N'$ induit un isomorphisme $N/(N \cap N') \rightarrow (N + N')/N$.

Si $N' \subset N \subset M$, le morphisme $M \rightarrow M/N'$ induit un isomorphisme $M/N \rightarrow (M/N')/(N/N')$.

Soit A un anneau ayant un unique idéal maximal P , M un A -module de type fini. Alors

- si $M = PM$ alors $M = 0$.

- Si $(v_i)_{1 \leq i \leq n}$ est une base de M/PM , et si (m_i) relève (v_i) , alors (m_i) est un système de générateurs de M . Les systèmes générateurs minimaux de M ont le même nombre d'éléments (non démontré).

Exercice: Si $a = 1 + b$ et b appartient à l'intersection des idéaux maximaux, alors a est inversible, i.e. $Aa = A$ (tout idéal propre est contenu dans un idéal maximal).

Cours 13 Comment reconnaître sur les coefficients d'un polynôme $P = a_n X^n + \dots + a_0 \in K[X]$ non constant si P a une racine double dans une clôture algébrique de K ? Par le discriminant $Discr(P) \in K$ qui pour un polynôme quadratique $aX^2 + bX + c$ est $b^2 - 4ac$. Le discriminant est nul si et seulement si P a une racine double.

Pour un polynôme cubique, $a_3 X^3 + a_2 X^2 + a_1 X + a_0$ le discriminant est $a_1 a_2^2 - 4a_0 a_2^3 - 4a_3 a_1^3 - 27a_0^2 a_3^2 + 18a_0 a_1 a_2 a_3$, le discriminant de $X^3 + bX + c$ est $-4b^3 - 27c^2$.

Comment reconnaître sur les coefficients de deux polynômes $P = a_n X^n + \dots + a_0, Q = b_m X^m + \dots + b_0 \in K[X]$ non constants si P, Q ont une racine commune dans une clôture algébrique de K ? Par le résultant $Res(P, Q) \in K$. Le résultant est nul si et seulement si P, Q ont une racine commune.

P, Q premiers entre eux dans $K[X]$ est équivalent à P, Q n'ont pas de racine commune dans K^a (Si une racine commune, alors $1 = 0$ by Bezout; si pas de racine commune, pas de facteurs communs).

Le résultant est le déterminant d'une matrice carrée $n \times m$, appelée la matrice de Sylvester de P, Q . Première ligne $(a_n, a_{n-1}, \dots, a_0, 0, \dots, 0)$, que l'on répète m fois en décalant vers la droite, puis la $m+1$ -ligne $(b_m, b_{m-1}, \dots, b_0, 0, \dots, 0)$, que l'on répète n fois en décalant vers la droite.

Matrice universelle: les coefficients $a_i = x_i, b_j = y_j$ sont des indéterminées, la matrice est à coefficients dans $R := \mathbb{Z}[x_i, y_j]$. Résultant universel.

Les lignes sont les coefficients de la colonne $C = (X^{m-1}P, \dots, P, X^{n-1}Q, \dots, Q)^t$ sur la base descendante $X^{m+n-1}, \dots, 1$ du R -module $Pol_{\leq m-1} \in R[X]$ des polynômes de degré $\leq n + m - 1$, i.e.

$C = X^{n+m-1}C_{m+n-1} + \dots + 1C_0$. Par Cramer,

$Res(P, Q) = \det(C_{m+n-1}, \dots, C_0) = \det(C_{m+n-1}, \dots, C_1, C) = fP + gQ$ pour $f, g \in R[X]$.

Si on spécialise $x_i \mapsto a_i, y_j \mapsto b_j : \mathbb{Z}[x_i, y_j] \rightarrow K$, le résultant est non nul si et seulement si $P = P_a, Q = Q_b$ sont premiers entre eux dans $K[X]$.

Définition du discriminant: $Res(P, P') = (-1)^{n(n-1)/2} a_n Discr(P)$. Noter que a_n divise la première colonne de la matrice de Sylvester de P, P' .

Lien coefficients racines. Si $P = a_n \prod_i (X - \alpha_i), Q = b_m \prod_j (X - \beta_j)$ scindés,

$Res(P, Q) = a_n^m b_m^n \prod_{1 \leq i \leq n, 1 \leq j \leq m} (\alpha_i - \beta_j)$.

$Res(P, P') = a_n^{2n-1} \prod_{i \neq j} (\alpha_i - \alpha_j)$ (écrire $P' = a_n \sum_j \prod_{i \neq j} (X - \alpha_i)$),

$Discr(P) = a_n^{2n-1} \prod_{i < j} (\alpha_i - \alpha_j)^2$.

La relation coefficients/racines se déduit de:

- le résultant est antisymétrique $Res(P, Q) = (-1)^{mn} Res(Q, P)$ (déterminant)

- Multiplication par un scalaire $Res(aP, Q) = a^m Res(P, Q)$ (déterminant)

- Multiplicatif $Res(P_1 P_2, Q) = Res(P_1, Q) Res(P_2, Q)$,

- $Res(X - a, Q) = Q(a)$.

La preuve des deux dernières propriétés (pour simplifier P, Q unitaires) se fait avec le "symbole de Legendre" pour les polynômes, $(\frac{P}{Q}) =$ déterminant de la multiplication par P dans $R[X]/QR[X]$.

- $Res(P, Q) = (-1)^{mn} (\frac{P}{Q})$.

Cette formule est très utile pour calculer le résultant. Comme $(\frac{P}{Q})$ ne dépend que du reste de la multiplication de P par Q , on peut faire baisser les degrés de P, Q en utilisant les autres propriétés.

$(f, g) \rightarrow fP + gQ, W \mapsto (r_Q(W), q_Q(W)) : Pol_{\leq m-1} \times Pol_{\leq n-1} \rightarrow Pol_{\leq m+n-1} \rightarrow Pol_{\leq m-1} \times Pol_{\leq n-1}$.

La matrice de la première application linéaire est la transposée de la matrice de Sylvester, la matrice de la seconde a pour déterminant $(-1)^{mn}$. La matrice de l'application composée $(f, g) \mapsto (r_Q(fP), g + q(fP))$ a le même déterminant que celui de l'application $f \mapsto r_Q(fP)$ i.e. $(\frac{P}{Q})$. Lorsque $Q = X - a$, l'image de 1 est $P(a)$. Donc $Res(P, X - a) = P(a)$. Par antisymétrie, $Res(X - a, Q) = Q(a)$.

Cours 14

$$(X - t_1) \dots (X - t_n) = X^n - s_1 X^{n-1} + \dots + (-1)^n s_n.$$

$s_i = s_i(t_1, \dots, t_n)$ i -ième fonction symétrique en $(t_1, \dots, t_n)$. s_i polynôme homogène de degré i .

$s_i(t_1, \dots, t_{n-1}, 0)$ est la i -ième fonction symétrique $s_{i,o}$ en $(t_1, \dots, t_{n-1})$ si $i \neq n$ et $s_n(t_1, \dots, t_{n-1}, 0) = 0$.

monôme $t_1^{k_1} \dots t_n^{k_n}$ de degré $d(k) := k_1 + \dots + k_n$ et de poids $p(k) := k_1 + \dots + n k_n$. Le polynôme $s_1^{k_1} \dots s_n^{k_n}$ est de degré $d = p(k)$ en $(t_1, \dots, t_n)$.

Partition de d associée: éléments $\leq n$.

Partition de d conjuguée: longueur $\leq n$.

Degré, poids d'un polynôme: maximum des degrés, poids des monômes.

A anneau commutatif, pour $s \in S_n$ et $P \in A[t_1, \dots, t_n]$ on note $P^s(t_1, \dots, t_n) = P(t_{s(1)}, \dots, t_{s(n)})$.

$$P^{ss'} = (P^s)^{s'}.$$

$P(t_1, \dots, t_n)$ symétrique implique $P_o := P(t_1, \dots, t_{n-1}, 0) \in A[t_1, \dots, t_{n-1}]^{S_{n-1}}$ symétrique.

$A[t_1, \dots, t_n]^{S_n}$ est un sous-anneau de $A[t_1, \dots, t_n]$.

Pour tout $f \in A[t_1, \dots, t_n]$ symétrique de degré $\leq d$, il existe $g \in A[s_1, \dots, s_n]$ de poids $\leq d$ tel que $f = g$. Preuve par induction on (n, d) .

Vrai $n = 1$. Supposons vrai pour $n - 1$ et soit $f \in A[t_1, \dots, t_n]$ symétrique de degré $\leq d$. Vrai pour $d = 1$. Supposons vrai pour degrés $< d$. Il existe $g_1 \in A[s_{1,o}, \dots, s_{n-1,o}]$ de poids $\leq d$ tel que $f_{\leq} = g_1$. Le polynôme $g_1(s_1, \dots, s_{n-1})$ est symétrique de degré $\leq d$ en $(t_1, \dots, t_n)$ et $f_1 = f - g_1(s_1, \dots, s_{n-1}) \in A[t_1, \dots, t_n]$ est symétrique de degré $\leq d$ et nul lorsque $t_n = 0$. Donc $f_1 = s_n f_2$ avec $f_2 \in A[t_1, \dots, t_n]$, qui est symétrique et de degré $\leq d - n$. Donc il existe $g_2 \in A[s_1, \dots, s_n]$ tel que $f_2 = g_2$. Prendre $g = g_1(s_1, \dots, s_{n-1} + s_n g_2(s_1, \dots, s_n))$.

Les fonctions symétriques sont algébriquement indépendantes: il n'existe pas de polynôme non nul $P \in A[X_1, \dots, X_n]$ tel que $P(s_1, \dots, s_n) = 0$ dans $A[t_1, \dots, t_n]$.

Recurrence sur n . Vrai $n = 1$. Supposons vrai $n - 1$. Si faux pour n , choisir P de degré minimal, et développer P en X_n . Le terme constant $f \in A[X_1, \dots, X_{n-1}]$ n'est pas nul car $s_n Q(s_1, \dots, s_n) = 0$ implique $Q(s_1, \dots, s_n) = 0$. Faire $t_n = 0$. Il ne reste que le terme constant $f(s_{1,o}, \dots, s_{n-1,o}) = 0$. Absurde par hypothèse de récurrence.

Exemple $\delta(t) = \prod_{i < j} (t_i - t_j)$ pas symétrique mais $\prod_{i < j} (t_i - t_j)^2$ symétrique, égal à $D(s_1, \dots, s_n)$ le discriminant du polynôme $X^n - s_1 X^{n-1} + \dots + (-1)^n s_n$.

$$A[t_1, \dots, t_n]^{S_n} = A[s_1, \dots, s_n] \simeq A[t_1, \dots, t_n].$$

Relations de Newton pour $p_d := t_1^d + \dots + t_n^d$ pour $d \geq 0$ (pas une base).

$$p_1 = s_1, p_2 = s_1 p_1 - 2s_2, p_3 = s_1 p_2 - s_2 p_1 + 3s_3, \dots,$$

$$p_d = s_1 p_{d-1} - s_2 p_{d-2} + \dots + (-1)^{d-2} s_{d-1} p_1 + (-1)^{d-1} s_d d \text{ si } d \leq n.$$

$$p_d = s_1 p_{d-1} - s_2 p_{d-2} + \dots + (-1)^{n-1} s_n p_{d-n} \text{ pour } d > n.$$

$A[t_1, \dots, t_n]$ est un module libre sur $A[t_1, \dots, t_n]^{S_n}$ de rang $n!$ de base $t_1^{k_1} \dots t_n^{k_n}$ avec $0 \leq k_i \leq i - 1$ pour $1 \leq i \leq n$. (Sans démonstration).

Cours 15

Polynôme irréductible séparable: $P \in Irr K[X]$ de racines simples dans une clôture algébrique K^a .

$X^p - T \in \mathbf{F}_p(T)[X]$ est irréductible (Eisenstein) non séparable (une seule racine d'ordre p dans $\mathbf{F}_p(T)^a$).

Corps parfait: tout polynôme irréductible est séparable (définition 1).

Exemple de corps parfait:

- corps algébriquement clos (un polynôme irréductible est de degré 1),
- corps de caractéristique 0 (la dérivée d'un polynôme non constant est non nulle de degré strictement inférieur, et un polynôme irréductible $P \in Irr K[X]$ de racine $\alpha \in K^a$ engendre l'idéal des polynômes $Q \in Irr K[X]$ tels que $Q(\alpha) = 0$)
- corps fini (même démonstration une fois que l'on sait que la dérivée d'un polynôme irréductible $P \in Irr K[X]$ est non nulle).

Corps parfait: de caractéristique 0 ou de caractéristique p avec un Frobenius surjectif (définition 2 qui implique la définition 1). Par comptage, un corps fini est un corps parfait. La dérivée d'un polynôme irréductible $P \in Irr K[X]$ est non nulle si le corps est parfait (en caractéristique $p > 0$, la dérivée d'un polynôme $Q \in K[X]$ est nulle si et seulement si $Q \in K[X^p]$. Si le Frobenius est surjectif, il existe $R \in K[X]$ tel que $Q = R^p$ donc Q ne peut être irréductible).

Si K est de caractéristique $p > 0$, les racines de $P \in \text{Irr}K[X]$ dans K^a ont même multiplicité p^k (Si P non séparable, alors $P = Q(X^p)$ pour $Q \in \text{Irr}K[X]$. Par induction, $P = Q(X^{p^k})$ pour $Q \in K[X]$ séparable).

Les prolongements à une extension monogène $K[\alpha]$ d'un morphisme $f : K \rightarrow L$ sont en bijection avec les racines dans L de l'image par f du polynôme minimal de α dans $K[X]$.

Déviage d'une extension finie E/K par des extensions monogènes.

Le nombre de K -automorphismes d'une extension finie E/K est majoré par le degré $[E : K]$.

La multiplication par $x \in E$ est une application K -linéaire $E \rightarrow E$. L'anneau des applications K -linéaires de E dans E est un E -espace vectoriel de dimension $[E : F]$

Indépendance linéaire des morphismes de corps $E \rightarrow L$ dans le L -espace vectoriel des applications de E dans L (famille finie liée $\sum_{i=1}^n a_i f_i = 0$ implique $\sum a_i f_i(x) f_i = 0$ pour tout $x \in E$, si n est minimal alors les f_i sont égaux donc $n = 1$, absurde).

Cours 16 Soit E/K un extension finie. On dit que E/K est galoisienne si $\text{Aut}_K E = [E : K]$.

Ceci est équivalent à: $\text{Aut}_K E$ est une base sur E de l'espace des applications K -linéaires $f : E \rightarrow E$ (qui contient E , via la multiplication $f_x : ? \rightarrow ?x$ pour $x \in E$). Autrement dit, toute application K -linéaire $f : E \rightarrow E$ s'écrit uniquement $f = \sum_{\sigma \in \text{Aut}_K E} a_\sigma \sigma$ avec $a_\sigma \in E$.

Ceci est aussi équivalent à $E^{\text{Aut}_K E} = K$ (l'ensemble des points fixes de $\text{Aut}_K E$ est K).

Exemples: une extension de corps finis, l'extension cyclotomique, une extension quadratique, sont galoisiennes, mais $\mathbb{Q}[2^{1/3}]/\mathbb{Q}$ n'est pas une extension galoisienne.

Théorème principal de la théorie de Galois. Soit E/K une extension finie de groupe de Galois $G := \text{Aut}_K E$. L'application $H \rightarrow E^H$ est une bijection entre les sous-groupes de G et les sous-extensions de E/K . L'extension E/E^H est galoisienne de groupe de Galois H . L'extension E^H/K est galoisienne ssi H est distingué dans G ; son groupe de Galois est alors G/H .

La démonstration du théorème principal utilise:

Soit G un groupe fini d'automorphismes d'un corps L . Alors l'ensemble L^G des points fixes de G est un corps, et l'extension L/L^G est finie de degré majoré par le cardinal $n = |G|$ de G .

Variante (finie) du théorème d'indépendance L -linéaire des K -morphisms d'une extension finie E/K dans un corps L . Si $\sigma_1, \dots, \sigma_r : E \rightarrow L$ sont r K -morphisms distincts, et $e_1, \dots, e_n$ est une base de E/K , alors les vecteurs $V(\sigma_1) = (\sigma_1(e_i))_{1 \leq i \leq n}, \dots, V(\sigma_r)$ de L^n sont L -linéairement indépendants.

Exercice: L'extension $\mathbb{Q}(2^{1/4})/\mathbb{Q}$ n'est pas galoisienne, pour trouver les sous-extensions, on considère l'extension galoisienne $\mathbb{Q}(2^{1/4}, i)/\mathbb{Q}$ et le sous-groupe H du groupe de Galois G de $\mathbb{Q}(2^{1/4}, i)/\mathbb{Q}$ de points fixes $\mathbb{Q}(2^{1/4})$. Les sous-extensions de $\mathbb{Q}(2^{1/4})/\mathbb{Q}$ sont les points fixes de $\mathbb{Q}(2^{1/4}, i)/\mathbb{Q}$ par les sous-groupes de G qui contiennent H .

Cours 17 Exercice du partiel: Pour $n > 2$, $\mathbb{Q}(e^{2i\pi/n})/\mathbb{Q}$ est galoisienne, de groupe de Galois commutatif, isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$, contient le corps $\mathbb{Q}(\cos(2\pi/n))$ qui est l'ensemble des éléments fixes de $\mathbb{Q}(e^{2i\pi/n})$ par la conjugaison complexe, est de degré $\phi(n)/2$ sur $\mathbb{Q}$, l'extension $\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}$ est galoisienne de groupe de Galois le quotient de $(\mathbb{Z}/n\mathbb{Z})^*$ par le sous-groupe d'ordre 2 engendré par la classe de -1 .

Corps des racines dans un polynôme $P \in K[X]$ non constant dans une clôture algébrique K^a . Construction abstraite par factorisation euclidienne de P et corps de ruptures successifs $E \subset E[X]/Q[X]E[X]$ pour $Q \in E[X]$ facteur irréductible de P de degré ≥ 2 .

Si les facteurs irréductibles de P ont leur racines simples (toujours vrai si K est parfait), le corps des racines de P est une extension galoisienne de K . Son groupe de Galois est appelé le groupe de Galois sur K de P .

Extension radicale finie: $K = E_0 \subset E_1 \subset \dots \subset E_r = E$ telle que $E_{i+1} = E_i(x_i^{1/n_i})$ pour $x_i \in E_i$ et n_i un entier ≥ 2 et $0 \leq i \leq r-1$.

Equation $P(X) = 0$ résoluble par radicaux: le corps des racines de P est une extension galoisienne radicale finie.

Cours 18 Groupe fini résoluble: filtration par des sous-groupes $1 \subset G_1 \subset \dots \subset G_i \subset G_{i+1} \subset \dots \subset G_n$ tels que G_i distingué dans G_{i+1} et le quotient G_{i+1}/G_i est abélien.

Un groupe quotient d'un groupe résoluble est résoluble.

Le groupe alterné A_5 n'est pas résoluble (sans démonstration).

Exercice. Un sous-groupe d'un groupe résoluble est résoluble. Le groupe symétrique S_4 est résoluble. Le groupe symétrique S_n n'est pas résoluble pour $n \geq n$.

Th. Une extension radicale finie est résoluble.

Soit p un nombre premier, et H un sous-groupe de S_p d'ordre divisible par p et contenant une transposition. Alors $H = S_p$ (sans démonstration).

Soit $P \in \mathbf{Z}[X]$ unitaire de degré p , admettant $p-2$ racines réelles exactement. Alors le groupe de Galois de P sur $\mathbf{Q}$ est S_p .

L'équation $P(X) = 0$ avec $P(X) = X^5 - 4X + 2$, n'est pas résoluble par radicaux.

Cours 19

$z \in \mathbf{C}$ constructible à la règle et au compas ssi le groupe de Galois du polynôme minimal de z sur $\mathbf{Q}$ est d'ordre une puissance de 2.

Un p -groupe fini est résoluble.

Un 2-groupe fini a une filtration de quotients d'ordre 2.

Quadrature du cercle

Trissection de l'angle: impossible pour $e^{2i\pi/9}$.

Un nombre premier p est "de Fermat" si $p = 2^n + 1$ pour un entier $n \geq 1$.

Racines de l'unité d'ordre n constructibles à la règle et au compas: $\phi(n)$ est une puissance de 2, équivalent à n est une puissance de 2 multiplié par des nombres premiers de Fermat distincts.

Un nombre premier de Fermat est de la forme $p = 2^{2^r} + 1$. Si $n = 2^r m$ avec $m \geq 3$ impair alors $2^n + 1$ est divisible par $2^{2^r} + 1 > 1$, car $X^m + 1$ est divisible par $X + 1$ dans $\mathbf{Z}[X]$.

Cours 20

A -module de torsion M : pour tout $m \in M$ non nul il existe $a \in A$ non nul tel que $am = 0$.

L'annulateur de m dans A est l'ensemble des $a \in A$ tels que $am = 0$. C'est un idéal. Il est non nul ssi m est de torsion.

Si $M = Am_1 + \dots + Am_r$ est de type fini et de torsion, alors il existe $a \in A$ non nul tel que $aM = 0$.

L'annulateur de M dans A est l'intersection des annulateurs des m_i .

Supposons A principal. On appelle période de M ou de $m \in M$ un générateur de son annulateur.

Un A -module cyclique Am est isomorphe à $A/(a)$ où a est une période de m , i.e. de Am .

P est un système de représentants des irréductibles modulo les unités de A .

Si $p \in P$, la période de pm est a si $(a, p) = 1$ et a/p si $p|a$.

Décomposition p -primaire d'un A -module de torsion de type fini sur un anneau principal.

Si M est de type fini, et $aM = 0$ on a déjà vu (lemme chinois) que M est une somme directe $M = \bigoplus_{p \in P} M_p$ où M_p est un A -module annulé par $p^{v_p(a)}$ (on dit que M_p est p -primaire).

M_p est de type fini (quotient de M de type fini). Si a est une période de M , alors $p^{v_p(a)}$ est une période de M .

Théorème. Soient A un anneau principal et M un A -module de torsion de type fini. Alors $M \simeq A/(a_1) \oplus \dots \oplus A/(a_r)$, $(0) \neq (a_1) \subset \dots \subset (a_r) \neq A$. La suite d'idéaux $(a_1) \subset \dots \subset (a_r) \neq A$ est unique.

Existence pour un module p -primaire $M = Am_o + Am_1 + \dots + Am_r$, $r \geq 1$ de période p^v , par induction sur le nombre de générateurs. On range de sorte que les annulateurs des m_i soient $(p^v) \subset \dots \subset (p^{v_r})$. Le module quotient M/Am_o a r générateurs. Par induction $M/Am_o = An_1 \oplus \dots \oplus An_s$.

La surjection $f: M \rightarrow M/Am_o$ a une section, i.e. une application A -linéaire $g: M/Am_o \rightarrow M$ telle que $fg(m') = m'$ pour tout $m' \in M/Am_o$. (La section existe, car chaque n_i se relève en un élément $z_i \in M$ de même période).

Pour tout anneau commutatif A , une application A -linéaire $f: M \rightarrow M'$ admettant une section $g: M' \rightarrow M$, fournit une somme directe $M = g(M') \oplus \text{Ker}(f) \simeq M' \oplus \text{Ker}(f)$ ($fg(m') = m'$ implique que g est injective et $g(M') \cap \text{Ker}(f) = 0$. D'autre part $gf(m) - m \in \text{Ker}(f)$).

Existence. La décomposition en modules p -primaire et le lemme chinois impliquent: Il existe $P' \subset P$ est fini et pour tout $p \in P'$ un ensemble $V_p \subset \mathbf{N}_{\geq 1}$ fini tel que

$$M \simeq \bigoplus_{p \in P', k \in V_p} A/(p^k) \simeq \bigoplus A/(a_1) \oplus \dots \oplus A/(a_r) \text{ avec } (a_1) \subset \dots \subset (a_r) \neq A.$$

Cours 21

Dictionnaire. $P(a)$ l'ensemble des $p \in P$ divisant a . Alors $P(a_1) = P'$ et $v_p(a_1)$ est le plus grand élément de V_p .

On a $M = A/(a_1) \oplus M_1$ avec $P'_1 \subset P'$ est l'ensemble des $p \in P'$ tel que $m_p \neq 1$ et $V_{p,1}$ pour $p \in P'_1$ est V_p privé de son plus grand élément.

$P(a_2) = P'_1$ et $v_p(a_2)$ est le plus grand élément de $V_{p,1}$, etc.

La suite $v_p(a_i)$ n'est pas nulle décroît pour $p \in P'$. Elle contient $r_p \leq r$ termes non nuls, et il existe $p \in P'$ tel que $r_p = r$.

L'unicité de la décomposition longue de M , i.e. de P' , $(V_p)_{p \in P'}$ est équivalente à celle de la décomposition courte de M , i.e. de $(a_1) \subset \dots \subset (a_r) \neq A$.

Preuve de l'unicité sur la décomposition courte de M .

$A/(a) \simeq A/(b)$ ssi $(a) = (b)$ (annulateurs).

Soit $M = Am_1 = A/Aa$ et $p \in P$. Alors $(a, p) = 1$ ss'il existe $\lambda, \mu \in A$ tel que $\lambda a + \mu p = 1$ ssi $\mu p m_1 = m_1$ ssi $m_1 \in pM$ ssi $M = pM$ ssi $M/pM = 0$.

Si $a = pb, b \in A$, alors l'application linéaire naturelle $A/(p) \rightarrow M/pM$ est un isomorphisme car $M/pM \neq 0$, A/pA est un corps.

N_i sous module de M_i alors $N = \oplus N_i$ est un sous-module de $M = \oplus M_i$ et $\oplus M_i/N_i \simeq M/N$.

Soit $p \in P$. Alors M/pM est un espace vectoriel sur $A/(p)$ de dimension le nombre de a_i divisibles par p . Le maximum est r (atteint si et seulement si $p \in P(a_r)$), donc r est canonique. Les ensembles $P(a_i)$ aussi.

Induction sur le nombre de facteurs irréductibles de $a = a_1 \dots a_r$. Si $a = p$, alors $r = 1$ et p est unique (déjà vu).

Sinon, soit $p \in P(a_r)$. Alors $pM = A/(a_1/p) \oplus A/(a_r/p)$. Comme a/p^r a moins de facteurs irréductibles (avec multiplicités) que a les a_i/p sont canoniques. Les a_i aussi.

Théorème. Soient A un anneau principal et M un A -module de torsion. Alors $M \simeq A^m \oplus A/(a_1) \oplus \dots \oplus A/(a_r)$, $(0) \neq (a_1) \subset \dots \subset (a_r) \neq A$. L'entier m et la suite d'idéaux $(a_1) \subset \dots \subset (a_r) \neq A$ sont uniques.

Pour tout anneau A , L, M deux A -modules avec L libre de base $e_1, \dots, e_n$, et $m_1, \dots, m_n \in M$, il existe une unique application A -linéaire $L \rightarrow M$ envoyant e_i sur m_i pour $1 \leq i \leq n$.

Toute application A -linéaire surjective dans un A -module libre est scindée.

A principal. Tout sous-module d'un A -module libre de rang fini est libre (Induction sur le rang, $n = 1$ vrai car A principal).

A principal. Tout A -module de type fini sans torsion est libre.

A principal. Le quotient d'un A -module de type fini M par son sous-module de torsion $M_{torsion}$ est libre de rang canonique m , M est isomorphe à $A^m \oplus M_{torsion}$, et $M_{torsion}$ est un A -module de type fini de torsion.