Université de Paris VI 2e semestre 2005-2006

Master de Mathématiques (M 20)

# THÉORIE DES NOMBRES

Daniel BERTRAND

Envoi 1/ Février 06

.

*Plan*

## Sommaire

Ce cours porte sur la théorie algébrique des nombres, certaines de ses applications en algorithmique et en cryptographie, et une introduction à la théorie analytique des nombres.

## Bibliographie

H. Cohen: *A course in computational number theory*; Springer, 1993.
M. Demazure: *Cours d'Algèbre*; Cassini, 1997.
G. Hardy and E. Wright: *An introduction to the theory of numbers*; Oxford UP, 1979
P. Samuel: *Théorie algébrique des nombres*; Hermann, 1967.
J-P. Serre: *Cours d'arithmétique*; PUF, 1970.

# CHAPITRE I

# EXTENSIONS ALGÉBRIQUES

## §1. Rappels sur les groupes. Fonction indicatrice d'Euler.

Un *groupe* est la donnée d'un ensemble $G$ muni d'une loi de composition interne : $G \times G \to G : (x, y) \mapsto xy$ associative, admettant un élément neutre, noté $e$, et tel que tout élément $x$ de $G$ admette un inverse, noté $x^{-1}$. $G$ est dit abélien (ou commutatif) si sa loi est commutative (on la note alors additivement). Le cardinal $|G|$ de $G$ s'appelle l'*ordre* de $G$ .

*Exemples* : le groupe symétrique $S_n$ formé des permutations d'un ensemble à $n$ éléments; $|S_n| = n!$; le sous-groupe $A_n \lhd S_n$ des permutations $s$ paires (i.e. de signature $\varepsilon_s = 1$);

$GL_n(\mathbf{R})$ = groupe multiplicatif des matrices réelles $n \times n$ inversibles;

le groupe additif $\mathbf{Z}$ des entiers rationnels; tout sous-groupe non nul de $\mathbf{Z}$ est de la forme $a\mathbf{Z}$, pour un unique entier rationnel $a > 0$ (effectuer des divisions euclidiennes par son plus petit élément $> 0$);

$\mathbf{Z}/a\mathbf{Z}$ = groupe additif des classes de congruence d'entiers rationnels modulo un entier rationnel $a > 0$; il est d'ordre $a$;

$(\mathbf{Z}/a\mathbf{Z})^*$ = groupe multiplicatif des classes de congruence modulo $a$ d'entiers $b$ premiers à $a$ (par Bézout, $(a, b) = 1$ ssi $\exists m, b' \in \mathbf{Z}, am + bb' = 1$, et $\overline{b'}$ est l'inverse de $\overline{b}$). Son ordre est noté $\phi(a)$ ($\phi :=$ *fonction indicatrice d'Euler*, avec $\phi(1) = 1$). Pour tout nombre premier $p$ et tout entier $n > 0$, $\phi(p) = p - 1$, $\phi(p^n) = p^{n-1}(p - 1)$, et on déduit du lemme chinois (cf. §2) que pour tout couple d'entiers $m, n$:

$$(m, n) = 1 \ \Rightarrow \ \phi(m, n) = \phi(m)\phi(n)$$

($\phi$ est une fonction arithmétique 'multiplicative'). Finalement, pour tout $a > 0$:

$$\phi(a) = a \prod_{p \text{ premier}, p|a} (1 - \frac{1}{p}).$$

Un *sous-groupe* $H$ de $G$ (notation : $H < G$ ) est une partie $H$ contenant $e$ , stable sous la loi de groupe de $G$ et sous l'inversion. Comme une intersection de sous-groupes

est un sous-groupe, on peut parler du plus petit sous-groupe $< S >$ de $G$ contenant une partie $S$ de $G$ , qu'on appelle aussi sous-groupe engendré par $S$ .

On appelle *classe (à gauche) modulo* $H$ toute partie de $G$ de la forme $xH := \{xh; h \in H\}$ pour un élément $x$ de $G$ , appelé représentant dans $G$ de la classe en question (chacun de ses éléments en est donc un représentant). Deux classes distinctes sont disjointes, et le cardinal de l'ensemble $G/H$ des classes modulo $H$, appelé *indice* de $H$ dans $G$ et noté $[G : H]$ , vérifie la relation :

$$|G| = |H| \times [G : H].$$

(En particulier, si $G$ est fini, $|H|$ divise $|G|$ .)

On dit que $H$ est distingué dans $G$ (ou normal; notation: $H \triangleleft G$), si $\forall x \in G, xH = Hx$ , i.e. $\forall h \in H, xhx^{-1} \in H$. L'ensemble $G/H$ est alors naturellement muni d'une structure de groupe, appelée *quotient* de $G$ par $H$ , telle que la surjection canonique $\pi : G \to G/H : x \mapsto (x) = xH$ est un homomorphisme (voir infra) de groupes. De plus, $\pi$ établit une bijection entre l'ensemble des sous groupes $A$ de $G$ contenant $H$ et l'ensemble des sous-groupes $A/H$ de $G/H$; pour $A \triangleleft G$, $A/H$ est normal dans $G/H$, et $(G/H)/(A/H) \simeq G/A$.

Un *homomorphisme* d'un groupe $G$ vers un groupe $G'$ est une application $f : G \to G'$ telle que $f(xy) = f(x)f(y)$ pour tout $(x, y) \in G \times G$ . (Alors $f(e) = e'; f(x^{-1}) = f(x)^{-1}$.) On parle d'endomorphisme si $G = G'$ , d'isomorphisme s'il existe un homomorphisme $g$ de $G'$ dans $G$ tel que $f \circ g = id_{G'}, g \circ f = id_G$, d'automorphisme si $f$ est à la fois un endo. et un iso..

**Proposition**: (décomposition canonique d'un homomorphisme) : *Soit $f$ un homomorphisme de $G$ vers $G'$ . Alors :*

*i) $Ker(f)$ = noyau de $f := \{x \in G : f(x) = e'\}$ est un sous groupe distingué de $G$ . Notons $\pi$ la surjection canonique de $G$ sur $G/Ker(f)$;*

*ii) $Im(f)$ = image def $:= \{f(x), x \in G\}$ est un sous-groupe de $G'$ . Notons $i$ l'injection canonique de $Im(f)$ dans $G'$ .*

*iii) il existe un unique isomorphisme $\overline{f}$ de $G/Ker(f)$ sur $Im(f)$ tel que $f = i \circ \overline{f} \circ \pi$.*

Soit $I$ un ensemble, et $\{G_i; i \in I\}$ une collection de groupes. On définit une structure de *groupe produit* sur le produit des ensembles $G_i$ en posant $(x_i)_{i\in I}.(y_i)_{i\in I} = (x_i y_i)_{i\in I}$. Si tous les $G_i$ sont égaux à un $G$ , ce groupe, noté $G^I$ (ou $G^n$ si $card(I) = n$ est fini), s'identifie au groupe des applications de $I$ dans $G$ .

On dit qu'un sous-groupe de $G$ est *cyclique* (ou monogène) s'il est engendré par un élément $x$ de $G$ . L'application $n \mapsto x^n$ définit alors un homomorphisme surjectif du groupe additif $\mathbf{Z}$ sur $< x >$, de noyau $a\mathbf{Z}$, avec $a \in \mathbf{Z}_{\geq 0}$, et $< x > \simeq \mathbf{Z}/a\mathbf{Z}$. Si $a$ est non

nul, $< x >= \{x, x^2, ..., x^{a-1}, x^a = e\}$ est un groupe fini, et son ordre $a$ s'appelle l'*ordre* de l'élément $x$ de $G$. En particulier, si $|G|$ est fini, l'ordre de tout élément de $G$ divise l'ordre de $G$. Appliqué au groupe $(\mathbf{Z}/a\mathbf{Z})^*$, ceci entraîne que pour tout entier $x$ premier à $a$, $x^{\phi(a)} \equiv 1 \pmod{a}$, et en particulier (petit théorème de Fermat):

$$\forall\ p \text{ premier}, \forall\ x \text{ t.q. } p \not| x\ :\ x^{p-1} \equiv 1 \bmod p.$$

Les générateurs d'un groupe cyclique fini $< x >$ d'ordre $a$ sont de la forme $x^b$, où $b$ est premier à $a$; il y en a donc $\phi(a)$. Soit alors $n$ un entier $> 0$. Pour tout diviseur $d = n/d'$ de $n$, il existe (exercice) un unique sous-groupe $C_d = d'\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/d\mathbf{Z}$ d'ordre $d$ du groupe cyclique $C_n = \mathbf{Z}/n\mathbf{Z}$. Par conséquent, les éléments d'ordre $d$ de $C_n$ sont les générateurs de $C_d$, et l'on a:

$$\forall n > 0,\ \Sigma_{d|n}\ \phi(d)\ =\ n.$$

La *fonction de Möbius* est l'application $\mu : \mathbf{Z}_{>0} \to \mathbf{Z}$ définie par $\mu(n) = 0$ si $n$ est divisible par un carré (i.e. par le carré d'un entier $> 1$); $\mu(n) = (-1)^r$ si $n$ est le produit de $r$ nombres premiers distincts (donc $\mu(1) = 1$). C'est une fonction arithmétique multiplicative, qui vérifie $\Sigma_{d|n}\mu(d) = 0$ pour tout $n \geq 2$. On en déduit: $\phi(n) = \Sigma_{d'|n}(\Sigma_{d|\frac{n}{d'}}\mu(d))\phi(d') = \Sigma_{dd'|n}\mu(d)\phi(d')$, soit

$$\forall n > 0,\ \phi(n)\ =\ \Sigma_{d|n}\ \mu(d)\frac{n}{d}.$$

*Application aux polynômes cyclotomiques*

**Lemme**: *soit $K$ un corps commutatif (cf. §2). Tout sous-groupe fini $G$ du groupe multiplicatif $K^*$ est cyclique.*

*Démonstation*: soit $d$ un diviseur de l'ordre $n$ de $G$ tel qu'il existe un élément $x$ d'ordre $d$ de $G$. Puisque $K$ est un corps comm., l'équation $X^d = 1$ a au plus $d$ solutions dans $K$, et tous les éléments d'ordre $d$ de $G$ sont des générateurs de $< x >$. Ainsi, pour tout $a|n$, il y a 0 ou $\phi(a)$ éléments d'ordre $a$ de $G$, et la formule $n = \Sigma_{a|n}\phi(a)$ impose qu'il y en ait $\phi(a)$ pour tout $a$. En particulier, il en existe d'ordre $n$, et $G$ est cyclique.

Soient $n$ un entier $> 0$, et $K$ un corps algébriquement clos de caractéristique nulle ou première à $n$ (cf. §2, ou prendre $K = \mathbf{C}$). Le polynôme $X^n - 1 \in K[X]$ est alors séparable (cf. fin du §2), et a $n$ racines distinctes dans $K$, qui forment le sous-groupe $\mu_n(K)$ de $K^*$ des racines $n$-ièmes de l'unité dans $K$. C'est un groupe d'ordre $n$, donc cyclique, dont les générateurs s'appellent les racines primitives $n$-ièmes de l'unité; ce sont les racines $n$-ièmes $\zeta$ vérifiant $\zeta^d \neq 1\ \forall d|n, d \neq n$. On appelle $n$-ième polynôme cyclotomique le polynôme, de degré $\phi(n)$:

$$\Phi_n(X)\ =\ \prod_{\zeta \in \mu_n(K),\ \zeta \text{ primitive}} (X - \zeta).$$

On a $\Pi_{d|n}\Phi_d(X) = X^n - 1$, et

$$\Pi_{d|n}(X^{\frac{n}{d}} - 1)^{\mu(d)} = \Pi_{d'|n}\Phi_{d'}^{\Sigma_{d|(n/d')}\mu(d)} \;=\; \Phi_n(X).$$

En particulier, $\Phi_n(X)$ est un polynôme unitaire à coefficients dans $\mathbf{Z}$ si $car(K) = 0$, et son image dans $\mathbf{F}_p[X]$ par réduction modulo $p$ si $car(K) = p$ est un nombre premier.

*Application à la cryptographie*

La système RSA de chiffrage à clef publique consiste à assigner à chaque membre $M_i$ d'un réseau $\{M_1, ..., M_n\}$ un couple $p_i, q_i$ de grands nombres premiers secrets, de produit $n_i = p_i q_i$ public, et un entier public $c_i$ premier à $\phi(n_i)$. Seul $M_i$ peut alors calculer l'inverse $d_i$ de $c_i$ dans $\mathbf{Z}/\phi(n_i)\mathbf{Z}$, car la connaissance de $\phi(n_i) = (p_i - 1)(q_i - 1)$ exigerait de factoriser $n_i$ (on peut alternativement supposer que $M_i$ a reçu $d_i$ en secret; en tous cas, une fois qu'il connaît $d_i$, $M_i$ peut oublier $p_i$ et $q_i$).

Un message est la donnée d'un entier $N$, inférieur à tous les $n_i$ (supposés du même ordre de grandeur) et tel que $(N, n_i) = 1$; en particulier, $N^{\phi(n_i)} \equiv 1 \pmod{n_i}$ pour tout $i$. Les dictionnaires "Entiers - Français; Français - Entiers" sont publics.

Si $M_1$ veut envoyer secrètement $N$ à $M_2$, il lui adresse de façon publique le reste $N_2$ de la division de $N^{c_2}$ par $n_2$. Pour récupérer $N$, $M_2$ calcule alors $N_2^{d_2} \equiv N \pmod{n_2}$, ce qu'ignorant $d_2$, les autres membres $M_i, i > 2$, du réseau ne sauront faire. Et s'ils tentent $N_2^{d_i}$ avec leur propre clef, l'incohérence du résultat obtenu leur montrera que le message ne leur était pas destiné.

Pour s'assurer que le message envoyé par $M_1$ lui est dû, on peut aussi procéder comme suit (on suppose ici que $n_1 < n_2$, de sorte que deux restes de division par $n_1$ distincts ne peuvent représenter la même classe modulo $n_2$): $M_1$ calcule le reste $N^1$ de la division de $N^{d_1}$ par $n_1$, et envoie $N_2^1 := (N^1)^{c_2} \pmod{n_2}$ à $M_2$. Alors, $M_2$ peut récupérer $N$ en calculant $(N_2^1)^{d_2} \equiv N^1 \pmod{n_2}$, puis $(N^1)^{c_1} \equiv N \pmod{n_1}$. La cohérence du message obtenu confirme que $M_1$ en était bien l'expéditeur.

## §2 Rappels sur les anneaux. Lemme chinois. PGCD.

Un anneau (unitaire) $A$ est un groupe abélien (de loi notée + , d'élément neutre 0), muni d'une loi de composition interne $A \times A \to A : (x, y) \mapsto xy$ associative, distributive par rapport à la loi + , admettant un élément neutre noté 1 . Si $x$ et $y$ commutent, on a la formule de Newton: $(x+y)^n = \Sigma_{k=0,..n}\ C_n^k\ x^k y^{n-k}$. On dit que $A$ est commutatif si tous ses éléments commutent entre eux, et que $A$ est *intègre* s'il est non nul et s'il n'a pas de diviseur de 0 autre que 0 (i.e. $xy = 0 \Rightarrow x = 0$ ou $y = 0$).

On appelle *unité* de $A$ tout élément $x$ de $A$ tel qu'il existe $y \in A$ vérifiant $xy = yx = 1$ ($y$ est alors unique, et noté $x^{-1}$). L'ensemble des unités de $A$ forme un groupe (pour la loi multiplicative), noté $A^*$. Un *corps* est un anneau non nul $K$ tel que $K^* = K \setminus \{0\}$.

*Exemples*: $M_n(\mathbf{R})$ = anneau (non commutatif pour $n > 1$ ) des matrices carrées réelles d'ordre $n$ ; alors, $(M_n(\mathbf{R}))^* = GL_n(\mathbf{R})$. Plus généralement, pour un anneau $A$ commutatif, $M_n(A)$ = anneau des matrices carrées d'ordre $n$ à coeff. dans $A$; alors $(M_n(A))^*$, noté $GL_n(A)$, est l'ensemble des matrices $x$ de déterminant

$$det(x) = \sum_{s \in S_n}\ \varepsilon_s x_{1,s(1)} ... x_{n,s(n)} \in A^*.$$

L'application $det : GL_n(A) \to A^*$ est un homomorphisme de groupes. On note $SL_n(A) = \{x \in M_n(A), det(x) = 1\}$ son noyau. Par exemple, $\mathbf{Z}^* = \{1, -1\}$, et $SL_n(\mathbf{Z})$ est un sous-groupe d'indice 2 de $GL_n(\mathbf{Z})$.

le groupe $\mathbf{Z}/a\mathbf{Z}$ est naturellement muni d'une structure d'anneau, dont le groupe des unités est le groupe noté $(\mathbf{Z}/a\mathbf{Z})^*$ au §1. Pour $a = p$ premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps, noté $\mathbf{F}_p$;

si $A_1$ et $A_2$ sont deux anneaux, on munit (en calculant coordonnée par coordonnée comme pour les groupes) le produit $A_1 \times A_2$ d'une structure d'anneau, non intègre si les $A_i$ sont non nuls. On a: $(A_1 \times A_2)^* = (A_1)^* \times (A_2)^*$;

l'anneau $A[X_1, ..., X_n]$ des polynômes en $n$ variables à coeff. dans un anneau commutatif intègre $A$ admet $A^*$ pour groupes des unités;

le corps des fractions $K = Fr(A)$ d'un anneau commutatif intègre $A$ est défini par les règles de calcul usuelles sur les fractions $\frac{a}{b}, a \in A, b \in A \setminus \{0\}$. On note $K(X_1, ..., X_n) := Fr(A[X_1, ..., X_n])$ le corps des *fractions rationnelles* en $n$ variables à coefficients dans $K$.

Un *idéal* (à gauche) $J$ de l'anneau $A$ est un sous-groupe du groupe $(A, +)$ tel que $\forall (a, x) \in A \times J, ax \in J$. Comme une intersection d'idéaux est un idéal, on peut parler du plus petit idéal $(S)$ de $A$ contenant une partie $S$ de $A$, qu'on appelle aussi idéal engendré par $S$ . Si $J = Ax := (x)$ est engendré par un élément $x$, on dit que J est un idéal principal. Un anneau $A$ est dit *principal* s'il est intègre et si tous ses idéaux sont principaux.

Pour tout idéal bilatère $J$ de $A$, le groupe quotient $A/J$ est naturellement muni d'une structure d'anneau, faisant de la surjection canonique $\pi : A \to A/J$ un homomorphisme d'anneau (voir infra). De plus, $\pi$ établit une bijection entre l'ensemble des idéaux de $A$ contenant $J$ et l'ensemble des idéaux de $A/J$.

Un *homomorphisme* d'un anneau $A$ vers un anneau $A'$ est une homo. de groupes additifs $f : A \to A'$ tel que $f(xy) = f(x)f(y)$ pour tout $(x, y) \in A \times A$, et $f(1) = 1'$. Endomorphisme, isomorphisme, automorphisme se définissent comme pour les groupes, et on a de même un théorème de décomposition canonique des homomorphismes d'anneaux (noter que $Ker(f)$ sera ici un idéal bilatère de $A$). Pour $A, A'$ commutatifs, on étend $f$ en un homomorphisme de $A[X]$ vers $A'[X]$ en associant à $P(X) = \Sigma_{i=0,..,n} a_i X^i \in A[X]$ le polynôme $f(P) = P^f := \Sigma_{i=0,...,n} f(a_i)X^i$ de $A'[X]$.

On suppose désormais nos anneaux *commutatifs*. Soient $J_1, ..., J_n$ des idéaux de $A$. On définit leur *produit* $J_1...J_n$ comme l'idéal *engendré par* les éléments de la forme $x_1...x_n$, où $x_i$ parcourt $J_i$ pour tout $i = 1, ..., n$. Leur intersection ensembliste $J_1 \cap ... \cap J_n$ est un idéal de $A$ , qui contient, en général strictement, $J_1...J_n$. L'ensemble $\{\Sigma_{i=1,...,n} x_i;\ \forall i,\ x_i \in J_i\}$ est un idéal de $A$, noté $J_1 + ... + J_n$. Dans ces conditions:

**Lemme chinois** : *Supposons que pour tout couple* $(i, j), 1 \leq i < j \leq n$, *d'indices distincts,* $J_i + J_j = A$. *Alors,* $J_1...J_n = J_1 \cap ... \cap J_n$, *et l'application* $\phi$ *qui, à un élément* $x$ *de* $A$, *associe l'élément* ($x$ mod $J_1, ..., x$ mod $J_n$) *de l'anneau produit des* $A/J_i$ *établit par passage au quotient un isomorphisme d'anneaux :*

$$A/J_1...J_n \simeq (A/J_1) \times ... \times (A/J_n).$$

*Démonstration.* Pour $r = 2$, soient $a_i \in J_i, i = 1, 2$ tels que $a_1 + a_2 = 1$, et $y \in J_1 \cap J_2$; alors, $y = ya_1 + ya_2 \in J_1J_2$, qui coïncide donc avec $J_1 \cap J_2$; pour tout couple $x_1, x_2$ d'élts de $A$, $\phi(a_1x_2 + a_2x_1) =$ (classe de $x_1$ mod $J_1$, classe de $x_2$ mod $J_2$), et $\phi$ est bien surjective. Pour $r > 2$, il existe par hypothèse $a_i \in J_i$ et $\alpha_i \in J_1$ tels que $\alpha_i + a_i = 1$ pour tout $i > 1$. Alors, $1 - a_2...a_r \in J_1$, donc $J_1 + J_2...J_r = A$, et on conclut par récurrence.

*Applications*: - $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ est isomorphe à $\mathbf{Z}/12\mathbf{Z}$ (et est en particulier un groupe cyclique). Mais $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ n'est pas cyclique (et n'est donc pas isomorphe à $\mathbf{Z}/9\mathbf{Z}$).

- soient $a_1, ..., a_n$ des entiers $\geq 1$, et premiers entre eux deux à deux (i.e. tels que $pgcd(a_i, a_j) = 1$ pour tout $i \neq j$). Alors, $(\mathbf{Z}/a_1...a_n\mathbf{Z})^* \simeq (\mathbf{Z}/a_1\mathbf{Z})^* \times ... \times (\mathbf{Z}/a_n\mathbf{Z})^*$. En particulier, la fonction indicatrice d'Euler est multiplicative (cf. §1).

On dit qu'un idéal $J$ d'un anneau $A$ est *maximal* (resp. *premier*) si $A/J$ est un corps (resp. un anneau intègre). Donc maximal $\Rightarrow$ premier (réciproque fausse en général: penser

à $\mathbf{C}[X,Y]$). $J$ est maximal ssi $J \neq A$ et le seul idéal le contenant strictement est $A$ tout entier; $J$ est premier ssi $J \neq A$ et $xy \in J \Rightarrow x \in J$ou $y \in J$. On peut déduire du lemme de Zorn (énoncé équivalent à l'axiome du choix) que tout idéal de $A$ distinct de $A$ est contenu dans un idéal maximal.

Soient $A$ un anneau *intègre*, et $a, b$ deux éléments de $A$. On dit que $a$ *divise* $b$ dans $A$ (notation : $a|b$) si $(a)$ contient $(b)$, qu'ils sont *associés* si $(a) = (b)$ (i.e. s'il existe une unité $u$ de $A$ telle que $a = ub$), que $a$ est *irréductible* si $a \neq 0, a \notin A^*$ et les seuls éléments de $A$ divisant $a$ sont les unités de $A$ et les éléments associés à $a$, et enfin que $a$ est *premier* si $(a)$ est un idéal premier non nul (i.e. $a \neq 0, a \notin A^*$ et $a|xy \Rightarrow a|x$ ou $a|y$). Tout élément premier est irréductible, mais l'inverse est faux en général (consider la relation $2.3 = (1+\sqrt{-5}).(1-\sqrt{-5})$ dans $A = \mathbf{Z}[\sqrt{-5}]$).

On dit qu'un anneau intègre $A$ est *factoriel* si tout élément non nul et non unité admet une décomposition en produit d'éléments irréductibles, *unique* à permutation et multiplications par des unités près.

**Proposition**: *soit $A$ un anneau intègre, et $a$ un élément de $A$ non nul et non unité.*

*i) si $A$ est factoriel, $a$ irréductible $\Leftrightarrow$ $a$ premier;*

*ii) $A$ principal $\Rightarrow$ $A$ factoriel;*

*iii) si $A$ est principal, tout idéal premier non nul est maximal, donc $a$ irréductible $\Leftrightarrow$ $a$ premier $\Leftrightarrow$ $(a)$ maximal.*

*iv) si $A$ admet un algorithme de division euclidienne, il est principal.*

Dans un anneau factoriel, on associe de la façon usuelle à toute famille $a_1, ..., a_n$ d'éléments (éventuellement nuls) de $A$ leur *pgcd* et leur *ppcm*, bien définis à multiplication par une unité près. On a $pgcd(a,b) \times ppcm(a,b) = ab$ (= signifiant ici associé). On dit que $a$ et $b$ sont *premiers entre eux* (ou: étrangers) si $pgcd(a,b) = 1$. L'idéal principal engendré par $pgcd(a,b)$ contient en général strictement l'idéal $(a,b)$. On a néanmoins bien égalité si l'anneau est principal, d'où , *dans un anneau principal*, la notation $(a,b) = 1$ pour dire que $a$ et $b$ sont premiers entre eux. Enfin, si $A$ est euclidien, l'algorithme de division euclidienne fournit un procédé de calcul effectif du pgcd.

Comme ils sont munis d'un algorithme de division euclidienne (de 'stathme' la valeur absolue pour l'un, le degré pour l'autre), les anneaux $\mathbf{Z}$ et $\mathbf{Q}[X]$ sont principaux. En revanche, $\mathbf{Z}[X]$ est seulement factoriel. On établira cette propriété au chapitre 5, en liaison avec d'utiles *critères d'irréductibilité*. Retenons dès à présent:

1) *Lemme de Gauss.*- Soit $A$ un anneau factoriel, et $P = a_o + a_1X + ... + a_nX^n$ un élément de $A[X]$. On appelle *contenu* de $P$ le pgcd $cont(P) = pgcd(a_0, ..., a_n)$ de ses coefficients. Pour

$P, Q$ dans $A[X]$, on a: $cont(PQ) = cont(P)cont(Q)$. En particulier, $A[X]$ est factoriel, et un élément $P$ de $\mathbf{Z}[X]$ est irréductible dans $\mathbf{Q}[X]$ si (et quand $cont(P) = 1$, seulement si) il est irréductible dans $\mathbf{Z}[X]$.

2) Soit $p$ un nombre premier, $\pi : \mathbf{Z}[X] \to \mathbf{F}_p[X]$ l'homomorphisme de réduction modulo $p$ (réduire modulo $p$ chacun des coefficients), et $P \in \mathbf{Z}[X]$ de coefficient dominant $a_n$ premier à $p$. Alors $P$ est irréductible dans $\mathbf{Q}[X]$ dès que $\pi(P)$ l'est dans $\mathbf{F}_p[X]$.

3) *Critère d'Eisenstein.*- Soit $P = a_o + a_1X + ... + a_nX^n \in \mathbf{Z}[X]$, et $p$ un nombre premier tel que $p \not| a_n, p|a_i$ pour $i < n, p^2 \not| a_0$; alors $P$ est irréductible dans $\mathbf{Q}[X]$.

On en déduit (poser $Y = X - 1$) que pour $p$ premier, le polynôme cyclotomique $\Phi_p(X) = 1 + X... + X^{p-1}$ est irréductible dans $\mathbf{Q}[X]$. L'irréductibilité, plus subtile, de tous les polynômes cyclotomiques $\Phi_n(X)$ dans $\mathbf{Q}[X]$ se déduit des résultats du chap. 3.

4) *Discriminant.*- Soient $K$ un corps, $P = a_nX^n + a_{n-1}X^{n-1} + ... + a_0 \in K[X]$ un polynôme de degré $n \geq 1$, de *polynôme dérivé* $DP(X) = \Sigma_{i=1,..,n} i a_i X^{i-1}$. On dit que $P$ est *séparable* si $(P, DP) = 1$. Alors (exercice), $P$ n'est pas divisible par un carré dans $K[X]$ (i.e. par le carré d'un élément non unité), et la réciproque est vraie quand $K$ est algébriquement clos. Ainsi, $P \in K[T]$ est séparable ssi il n'admet pas de racine multiple dans la clôture algébrique de $K$ (ou dans son corps de décomposition sur $K$, cf. §3).

De plus, il existe une expression polynômiale 'universelle' $D_n(a_0, ..., a_{n-1}, a_n)$ à coefficients dans $\mathbf{Z}$ (dont la valeur dans $K$ s'appelle le discriminant $Disc(P)$ de $P$), telle que, toujours sous l'hypothèse $a_n \neq 0$: $(P, DP) \neq 1 \Leftrightarrow Disc(P) = 0$. Par exemple,

$$Disc(X^n + a_1X + a_0) = (-1)^{n(n-1)/2}((1-n)^{n-1}a_1^n + n^n a_0^{n-1}).$$

Un homomorphisme d'anneaux dont la source est un corps, est injectif ou nul. Si $K$ est un corps, le noyau de l'homomorphisme de $\mathbf{Z}$ dans $K$ défini par $n \mapsto n.1$ est un idéal premier de $\mathbf{Z}$, donc égal à 0, ou à $p\mathbf{Z}$, pour un nombre $p$ premier. On dit respectivement que $K$ est de *caractéristique* nulle, ou égale à $p$. Dans ce deuxième cas, $K$ contient le corps $\mathbf{F}_p$, et l'application

$$F : K \to K : x \mapsto x^p$$

est un endomorphisme d'anneau, induisant l'identité sur $\mathbf{F}_p$ (d'après Fermat), et appelé *Frobenius* de $K$ (cf. chapitre 2). Si $car(K) = 0$, tout élément irréductible $P$ de $K[X]$ vérifie $(P, DP) = 1$, et est donc séparable. Si $car(K) = p$, il en est de même quand le Frobenius de $K$ est un automorphisme de $K$ (par exemple, pour $K = \mathbf{F}_p$): en effet, un élément $P$ irréductible non séparable vérifie $DP = 0$, donc $\exists S \in K[X]$ tel que $P(X) = S(X^p) = ((F^{-1}(S))(X))^p$, qui n'est pas irréductible dans $K[X]$. Mais si $F$ n'est pas surjectif sur $K$, il existe des polynômes irréductibles non séparables (cf. chapitre 3).

## §3. Extensions algébriques

Soit $K$ un corps (commutatif). On appelle *extension* de $K$ la donnée d'un corps $L$ et d'un homomorphisme d'anneaux (unitaires) $i$ de $K$ dans $L$. Comme $K$ est un corps, $i$ est nécessairement injectif, et on identifie en général $K$ à $i(K)$, en notant simplement $L/K$ une telle extension.

La multiplication des éléments de $L$ par ceux de $i(K)$ munit $L$ d'une structure naturelle d'espace vectoriel sur $K$ . La dimension (éventuellement infinie) de $L$ en tant que $K$-esp. vect. est appelée *degré* de l'extension $L/K$, et est notée $[L : K]$ (ne pas confondre avec l'indice d'un sous-groupe). On dit qu'une extension est *finie* si son degré l'est.

On appelle extension intermédiaire $M$ de $L/K$ la donnée de deux extensions $M/K$ et $L/M$ telles que la composée des injections sous-entendues correspondantes soit l'injection sous-entendue de $L/K$. Pour toute partie $S$ de $L$ , on désigne par $K[S]$ le sous-anneau de $L$ engendré par $K$ et $S$, et par $K(S) = Fr(K[S])$ l'extension intermédiaire de $L/K$ engendrée par $K$ et $S$ dans $L$. Si $S = \{s\}$ est réduite à un élément, on dit que $K(s)$ est une extension *monogène*. Si $S$ est fini, on dit que $K(S)/K$ est une extension *de type fini* (mais $K(S)/K$ ne sera pas forcément une extension finie; exemple: $S = \{T\}$ dans le corps $K(T)$ des fractions rationnelles à coefficients dans $K$.)

**Théorème 1**: *Soient $L/K$ une extension, et $M$ une extension intermédiaire. Alors,* $[L : K] = [L : M][M : K]$.

*Démonstration*: dans le cas où $[M : K] = m$ et $[L : M] = n$ sont finis, soit $\{\alpha_1, ..., \alpha_m\}$ (resp. $\{\beta_1, ..., \beta_n\}$) une base de $M$ de $K$ (resp. de $L$ sur $M$). Alors, la famille $\{\alpha_i\beta_j; 1 \leq i \leq m, 1 \leq j \leq n\}$ forme une base de l'espace vectoriel $L$ sur $K$, qui a donc pour dimension $mn$. Même argument dans le cas où une des extensions est infinie, en remplaçant les entiers $m, n$ par des cardinaux.

*Application* (exercices): le problème de trisection de l'angle ou de la duplication du cube ne peut être résolu par des constructions à la règle et au compas.

Soit $L/K$ une extension, et $\alpha$ un élément de $L$. L'ensemble

$$J_\alpha = \{P \in K[T],\ P(\alpha) = 0 \text{ dans } L\}$$

est un idéal de l'anneau pricipal $K[T]$, distinct de $K[T]$. Si $J_\alpha = 0$, i.e. si $\alpha$ ne vérifie aucune relation polynômiale non triviale à coefficients dans $K$, on dit que $\alpha$ est *transcendant* sur $K$. Sinon, on dit que $\alpha$ est algébrique sur $K$; l'idéal $J_\alpha$, distinct de 0 et de $K[T]$, admet alors un générateur unitaire de degré $\geq 1$, appelé *polynôme minimal* de $\alpha$ sur $K$, et noté $Min_{\alpha,K}$ (ou $M_\alpha$ si la référence à $K$ est claire); son degré s'appelle le *degré* de $\alpha$ sur $K$.

**Théorème 2**: *i) Soient $L/K$ une extension, et $\alpha$ un élément de $L$ algébrique sur $K$. Alors, $Min_{\alpha,K}$ est irréductible dans $K[T]$, de degré $n = [K(\alpha) : K]$, l'extension $K(\alpha)/K$ admet $\{1, \alpha, ..., \alpha^{n-1}\}$ pour base sur $K$, et $K(\alpha) = K[\alpha]$.*
*ii) Soit $P \in K[T]$, irréductible et unitaire. Alors, il existe une extension $M/K$ et un élément $\alpha$ de $M$ tels que $P = Min_{\alpha,K}$ et $M = K(\alpha)$. Une telle extension est appelée corps de rupture de $P$.*

*Démonstration*: i) soit $ev_\alpha : K[T] \to L : Q \mapsto Q(\alpha)$ l'homomorphisme d'anneau 'évaluation en $\alpha$'. Par passage au quotient par son noyau $J_\alpha$, il définit un isomorphisme de $K[T]/J_\alpha$ sur un sous-anneau (forcément intègre) de $L$, donc $J_\alpha$ est un idéal premier, non nul, donc maximal ((cf. §2, Proposition, iii). Ainsi, son générateur $M_\alpha$ est irréductible et $K[T]/J_\alpha$ est un corps, dont l'image $K[\alpha]$ par $ev_\alpha$ coïncide donc avec $K(\alpha)$, et est un espace vectoriel sur $K$ de dimension $n$, engendré par les images de $1, T, ..., T^{n-1}$.

ii) l'anneau $M = K[T]/(P)$ est un corps si $P$ est irréductible, et la classe $\alpha$ de $T$ modulo $(P)$ vérifie les conditions souhaitées.
[Dans la pratique, on calcule l'inverse d'un élément $\beta \neq 0$ de $M$, donné sous la forme $\beta = Q(\alpha)$, avec $P \not| Q$, en appliquant Bézout: $\exists\ A, Q' \in K[T], AP + QQ' = 1$; alors $\beta^{-1} = Q'(\alpha)$.]

Un *homomorphisme* d'une extension $(i, L)$ de $K$ vers une extension $(i', L')$ de $K$ est un homomorphisme d'anneau $\phi : L \to L'$ tel que $\phi o i = i'$. On dit alors que $\phi$ est un $K$-homomorphisme de $L$ vers $L'$ (ou: un homomorphisme de $L/K$ vers $L'/K$; comme $\phi$ est injectif, on parle aussi de *plongement* au lieu d'homomorphisme). Plus généralement, si $\phi$ est un homomorphisme de $K$ vers un corps $K'$, et $(i, L)$ (resp. $(i', L')$ une extension de $K$ (resp. $K'$), un homomorphisme d'anneau $\psi : L \to L'$ tel que $\psi o i = i' o \phi$ s'appelle un homomorphisme de $L$ vers $L'$ *au-dessus* de $\phi$ (ou: étendant $\phi$). Idem pour les iso., les endo., les automorphismes.

Le théorème de prolongement suivant entraîne en particulier que pour $P \in K[T]$ irréductible donné, tous les corps de rupture de $P$ sont $K$-isomorphes.

**Théorème 3** : *soient $K, K'$ deux corps, $\phi$ un homomorphisme de $K$ dans $K'$, $L/K, L'/K'$ deux extensions, et $\alpha$ un élément de $L$ algébrique sur $K$.*

*i)* (1er théorème de prolongement) *Soit $\alpha' \in L'$ algébrique sur $K'$, tel que $\phi(Min_{\alpha,K}) = Min_{\alpha',K'}$. Alors, il existe un unique homomorphisme $\psi$ de $K(\alpha)$ dans $L'$ au-dessus de $\phi$ tel que $\psi(\alpha) = \alpha'$.*

*ii) Soit $\psi$ un homomorphisme de $K(\alpha)$ dans $L'$ au-dessus de $\phi$. Alors, $\alpha' := \psi(\alpha)$ est algébrique sur $\phi(K)$ (donc sur $K'$), et vérifie $Min_{\alpha',\phi(K)} = \phi(Min_{\alpha,K})$.*

[Le nombre d'homomorphismes distincts de $K(\alpha)$ dans $L'$ au dessus de $\phi$ est donc égal au nombre de racines distintes de $\phi(Min_{\alpha,K})$ dans $L'$. ]

*Démonstration*: i) l'homomorphisme d'évaluation $Q \in K[T] \mapsto (\phi(Q))(\alpha') \in L'$ passe au quotient $K[T]/J_\alpha$ par son noyau, et induit un plongement $\psi : K(\alpha) \to L'$ envoyant $\alpha$ sur $\alpha'$, et dont la restriction à $K$ vaut $\phi$. Cela détermine entièrement $\psi$ sur $K(\alpha)$.

ii) $(\phi(Min_{\alpha,K}))(\alpha') = \psi(Min_{\alpha,K}(\alpha)) = 0$, et l'homomorphisme d'anneau $\phi : K[T] \to \phi(K)[T]$ préserve l'irréductibilité.

On dit qu'une *extension $L/K$ est algébrique* si *tous* ses éléments sont algébriques sur $K$; elle est dite transcendante dans le cas contraire (i.e. s'il existe un élement de $L$ transcendant sur $K$). Dans le cas d'une extension monogène, les propriétés suivantes sont équivalentes: $K(\alpha)/K$ est algébrique $\Leftrightarrow$ $K(\alpha)/K$ est finie $\Leftrightarrow$ $K[\alpha] = K(\alpha)$. D'où pour une extension quelconque:

$$L/K \text{ est finie} \Leftrightarrow L/K \text{ est algébrique } \textit{et} \text{ de type fini.}$$

Soient $L/K$ une extension, et $x, y \in L$ algébriques sur $K$. Alors, $K(x,y)/K$ est une extension finie (de degré $\leq [K(x) : K].[K(y) : K]$), donc algébrique. En particulier, $x+y$ et $xy$ sont algébriques sur $K$. Ainsi, *l'ensemble des éléments de $L$ algébriques sur $K$ forme un sous-corps de $L$*, appelé fermeture algébrique de $K$ *dans* $L$. C'est évidemment un extension algébrique de $K$, mais elle n'est pas nécessairement finie (exemple: la fermeture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$ dans $\mathbf{C}$). Par ailleurs, elle est sa propre fermeture algébrique dans $L$. En effet, pour toute extension intermédiaire $L/M/K$ , avec $M/K$ *algébrique, tout $x \in L$ algébrique sur $M$ est algébrique sur $K$* (si $S$ désigne l'ensemble des coefficients de $Min_{x,M}$, $x$ est algébrique sur $K(S)$, et $K(S,x)/K$ est une extension finie, donc algébrique.)

On dit qu'un corps $\Omega$ est *algébriquement clos* si les éléments irréductibles de $\Omega[T]$ sont tous de degré 1, i.e. si tout polynôme de degré $\geq 1$ admet une racine dans $\Omega$ (tout polynôme se décompose alors en facteurs linéaires dans $\Omega$). On dit qu'une extension $\overline{K}/K$ est une *clôture algébrique de $K$* si les deux conditions suivantes sont simultanément réalisées: $\overline{K}/K$ est une extension algébrique et $\overline{K}$ est un corps algébriquement clos.

**Théorème**: *tout corps $K$ admet une clôture algébrique $\overline{K}$. De plus, deux clôtures algébriques de $K$ sont $K$-isomorphes.*

*Démonstration*: nous nous contentons ici de vérifier l'existence d'une clôture algébrique en supposant qu'on dispose d'une extension $\Omega$ de $K$ algébriquement close, mais peut-être transcendante (grâce à l'Analyse ou la Topologie, c'est le cas de $K = \mathbf{Q}$, avec $\Omega = \mathbf{C}$). Soient donc $\overline{K}$ la fermeture algébrique de $K$ dans $\Omega$, $F$ un élément de $\overline{K}[T]$ et $\omega$ une racine

de $P \in \Omega[T]$ dans le corps alg. clos $\Omega$. Comme on vient de le voir, $\omega$ appartient à $\overline{K}$, qui est donc à la fois algébrique sur $K$ et algébriquement clos.

Soit $F \in K[T]$ un polynôme de degré $n \geq 1$, non nécessairement irréductible, de terme dominant $a_n$. On dit qu'une extension $L/K$ est un *corps de décomposition* de $F$ sur $K$ s'il existe $n$ éléments (non nécessairement distincts) $\alpha_1, ..., \alpha_n$ de $L$ tels que les deux conditions suivantes soient simultanément réalisées:

$$L = K(\alpha_1, ..., \alpha_n) \text{ et } F(T) = a_n \Pi_{i=1,...,n}(T - \alpha_i) \text{ dans } L[T].$$

La première condition entraîne alors que $L/K$ est une extension finie. On exprime la seconde en disant que $F$ se décompose en facteurs linéaires dans $L$, ou, plus simplement, qu'il *se décompose* (sous-entendu: complètement) dans $L$.

**Théorème 4**: *Soient $K$ un corps, et $F$ un élément de $K[T]$ de degré $n \geq 1$.*

*i) $F$ admet un corps de décomposition $L$ sur $K$.*

*ii)* (2ème théorème de prolongement) *Soient $\phi : K \to K'$ un homomorphisme, et $L'$ une extension de $K'$ dans laquelle $\phi(F)$ se décompose en facteurs linéaires. Alors, il existe un homomorphisme (non unique) $\psi$ de $L$ dans $L'$ au-dessus de $\phi$. De plus:*

*iii) Si $\phi$ est un isomorphisme, et si $L'$ est un corps de décomposition de $\phi(F)$ sur $K'$, alors, $\psi$ est un isomorphisme.*

[Deux corps de décomposition de $F$ sur $K$ sont donc $K$-isomorphes, et on peut parler, à $K$-isomorphisme près, 'du' corps de décomposition de $F$ sur $K$.]

*Démonstration.* i) C'est clair pour $n = 1$, et on procède par récurrence sur $n$ (sans fixer $K$). Supposons que $F$ ne se décompose pas en facteurs linéaires sur $K$. Il admet alors un facteur $M_1$ irréductible sur $K$ de degré $> 1$. D'après le théorème 2, il existe $K_1/K$ et $\alpha_1 \in K_1$ racine de $M_1$ tels que $K_1 = K(\alpha_1)$, de sorte que $F(T)$ s'écrit $(T - \alpha_1)F_1(T)$ dans $K_1[T]$. On conclut en appliquant l'hypothèse de récurrence au couple $(F_1, K_1)$.

ii) Par récurrence sur $n$. Soit $\phi(F) = \phi(a_n)\Pi_{i=1,...,n}(T - \beta_i)$ la décomposition de $\phi(F)$ dans $L'$, et $M_1$ le polynôme minimal de $\alpha_1$ sur $K$, de degré $r \leq n$. Après réindexation, on peut écrire $\phi(M_1) = \Pi_{i=1,...,r}(T - \beta_i)$ et $\phi(M_1)$, irréductible sur $\phi(K)$, est le polynôme minimal de $\beta_1$ sur $\phi(K)$. D'après le théorème 3.i, il existe un homomorphisme $\phi_1$ de $K_1 = K(\alpha_1)$ dans $L'$ au-dessus de $\phi$ envoyant $\alpha_1$ sur $\beta_1$. On conclut en appliquant l'hypothèse de récurrence à $F_1(T) := F(T)/(T - \alpha_1) \in K_1[T])$, $\phi_1 : K_1 \to K_1' = K'(\beta_1)$.

iii) Soient $\phi(F) = \phi(a_n)\Pi_{i=1,...,n}(T - \beta_i)$ la factorisation de $\phi(F)$ dans le corps de décomposition $L' = K(\beta_1, ..., \beta_n)$, et $\psi$ un homomorphisme de $L$ dans $L'$ au-dessus de $\phi$. D'après le théorème 3.ii, $\psi$ envoie les $\alpha_i$ sur certains des $\beta_j$ et par injectivité, préserve les multiplicités. Donc tous sont atteints, et $\psi$ est un isomorphisme.

# CHAPITRE II

# CORPS FINIS

## §1. Les corps $\mathbf{F}_q$.

Soient $p$ un nombre premier, et $K$ un corps de caractéristique $p$. Comme on l'a vu, $K$ contient $\mathbf{F}_p$, et est donc une extension de $\mathbf{F}_p$. Dans ces conditions, $K$ est un corps fini (c'est-à-dire: possède un nombre fini $q$ d'éléments), si et seulement si l'extension $K/\mathbf{F}_p$ est finie (c'est-à-dire: est de degré $d$ fini). Le $\mathbf{F}_p$-espace vectoriel $K$ a alors $q = p^d$ éléments. Ainsi un corps fini a pour cardinal une puissance pure de sa caractéristique (noter qu'un corps fini est forcément de caractéristique $\neq 0$). Inversément:

**Théorème 1**: *soient $q = p^d$ une puissance de $p$. Le corps de décomposition du poly. $G_d(T) = T^{p^d} - T$ sur $\mathbf{F}_p$ est, à isomorphisme près, l'unique corps de cardinal $q$. On le note $\mathbf{F}_q$.*
[Remarque: pour $d > 1$, il n'y a aucun rapport entre $\mathbf{F}_{p^d}$ et $\mathbf{Z}/p^d\mathbf{Z}$: le premier est un corps, le deuxième un anneau non intègre; le groupe additif de $\mathbf{Z}/p^d\mathbf{Z}$ est cyclique, celui de $\mathbf{F}_{p^d}$ un produit de $d$ groupes cycliques.]

La démonstration du théorème 1 repose sur le

**Lemme 1**: *Soit $K$ un corps fini, et $p^n$ son cardinal. Alors,*
*i) le Frobenius $F$ de $K$ est un automorphisme de $K$, qui vérifie $F^n = id_K$; en particulier, tout élément irréductible de $K[T]$ est séparable.*
*ii) pour tout entier $m \geq 1$, le polynôme $G_m(X) = X^{p^m} - X$ est séparable (ses racines dans toute extension de $K$ sont donc simples), et pour $m = n$, $G_n(T) = \Pi_{x \in K}(T - x)$.*

*Démonstration.* i) Rappelons (I, §2) que le Frobenius de $K$ est l'application $F : x \mapsto x^p$. C'est bien un endomorphisme de l'anneau $K$, puisque $F(xy) = (xy)^p = F(x)F(y)$, $F(1) = 1$, et $F(x + y) = \Sigma_{k=0,...,p} C_p^k x^k y^{p-k} = x^p + y^p = F(x) + F(y)$ (noter que $\forall k = 1, ..., p-1, p | C_p^k$). Comme sa source $K$ est un corps, $F$ est injectif, et donc surjectif puisque c'est un endomorphisme du groupe fini $(K, +)$. Ainsi, $F$ est un automorphisme. Comme le groupe multiplicatif $K^*$ est d'ordre $p^n - 1$, ses éléments $x$ vérifient $x^{p^n - 1} = 1$, d'où

pour tout $x \in K, F^n(x) = x^{p^n} = x = id_K(x)$. (NB: le fait que $F^n$ est l'identité entraîne d'ailleurs directement que $F$ est un automorphisme.) Comme $F$ est un automorphisme de $K$, la deuxième assertion résulte de I, fin du §2.

ii) La première assertion est claire ($DG_m(X) = -1$ est premier à $G_m$), et on vient de voir que les $p^n = deg(G_n)$ éléments de $K$ sont racines de $G_n$.

*Démonstration* du théorème 1. Soient $L$ le corps de décomposition du polynôme $G_d(T)$ sur $\mathbf{F}_p$, $F$ son Frobenius, et $M$ l'ensemble des racines de $G_d$ dans $L$. Par définition, $L$ est le sous-corps de $L$ engendré sur $\mathbf{F}_p$ par l'ensemble $M$. Mais on vérifie à la main (ou en disant que c'est l'ensemble des éléments $x$ de $L$ tels que l'automorphisme $\sigma = F^d$ de l'extension $L/\mathbf{F}_p$ vérifie $\sigma(x) = x$) que $M$ est lui-même un corps. Donc $M = L$. Par ailleurs, $M$ a $q$ éléments, puisque $G_d$ est un polynôme séparable, et $L$ est bien un corps fini à $q$ éléments. Enfin, d'après le Lemme 1.ii), tout corps $K$ de cardinal $q = p^d$ est un corps de décomposition du polynôme $G_d$ sur $\mathbf{F}_p$, et est donc isomorphe à $L$.

Fixons une clôture algébrique $\overline{\mathbf{F}}_p$ de $\mathbf{F}_p$. Le théorème 1 entraîne que pour tout entier $d$, il y a une et une seule extension $\mathbf{F}_{p^d}$ de $\mathbf{F}_p$ de degré $d$ contenue dans $\overline{\mathbf{F}}_p$: le corps $\mathbf{F}_p(\zeta)$ engendré par une racine primitive $(p^d-1)$-ième de l'unité dans $\overline{\mathbf{F}}_p$. (Rien de tel, bien sûr, pour $\overline{\mathbf{Q}}$, qui contient pour tout $d > 1$, une infinité d'extensions de $\mathbf{Q}$ de degré $d$, deux à deux non isomorphes.) Ces extensions s'imbriquent de la façon suivante, qui permet d'ailleurs de définir $\overline{\mathbf{F}}_p$ comme la réunion croissante des corps $\mathbf{F}_{p^{n!}},\ n \geq 1$.

**Proposition 1**: *soient $n$ et $m$ deux entiers $\geq 1$. Alors, $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m}$ si et seulement si $n|m$.*

*Démonstration*: si $\mathbf{F}_{p^m}$ est une extension de $\mathbf{F}_{p^n}$, son degré $d$ vérifie $p^m = (p^n)^d$, donc $m = dn$. Inversément, si $n|m$, $p^n - 1$ divise $p^m - 1$, donc $\mu_{p^n-1}(\overline{\mathbf{F}}_p) \subset \mu_{p^m-1}(\overline{\mathbf{F}}_p)$.

*Remarque* 1: considérons, avec les notations $m = dn$ précédentes, le $n$-ième itéré $F^n$ du Frobenius de $\mathbf{F}_{p^m}$. D'après le lemme 1, c'est un élément du groupe $G = Aut(\mathbf{F}_{p^m}/\mathbf{F}_{p^n})$ des automorphismes de l'extension $\mathbf{F}_{p^m}/\mathbf{F}_{p^n}$, i.e. des automorphismes du corps $\mathbf{F}_{p^m}$ induisant l'identité sur $\mathbf{F}_{p^n}$. On déduit des résultats du Chap. 3 que $G$ est un groupe cyclique, d'ordre $d$, engendré par l'automorphisme $F^n$. (Voir feuilles TD pour une preuve directe.)

En particulier, pour tout entier $m$, le groupe $Aut(\mathbf{F}_{p^m}/\mathbf{F}_p) \simeq \mathbf{Z}/m\mathbf{Z}$ est engendré par le Frobenius $F$ de $\mathbf{F}_{p^m}$. On peut néanmoins montrer que $Aut(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ est beaucoup plus gros que le groupe cyclique (isomorphe à $\mathbf{Z}$) qu'y engendre le Frobenius de $\overline{\mathbf{F}}_p$.

*Remarque* 2: On dit qu'une extension algébrique $L/K$ est *séparable* si pour tout $\alpha \in L$, le polynôme $Min_{\alpha,K}$ est séparable. Soit alors $K$ un corps *fini*. Le lemme 1 entraîne que

toute extension algébrique $L/K$ est séparable; si de plus $L/K$ est une extension finie, on a vu qu'il existe un élément $\zeta$ de $L$ tel que $L = K(\zeta)$. Ainsi, toute extension finie d'un corps fini est monogène. Plus généralement, on montrera au chapitre 3 que pour tout corps $K$, toute extension finie et séparable de $K$ est monogène. En revanche, le corps $K = \mathbf{F}_p(X)$, de caractéristique $p$ mais infini, admet des extensions finies non séparables (example: $L$ = le corps de rupture du polynôme $P(T) = T^p - X$, qui est irréductible sur $K$ mais est une puissance $p$-ième dans $L[T]$), tandis que le corps $K = \mathbf{F}_p(X, Y)$ admet même des extensions finies non monogènes (exemple: $L$ = le corps de décomposition du polynôme $F(T) = (T^p - X)(T^p - Y)$ sur $K$).

## §2. La loi de réciprocité quadratique.

Soit $p$ un nombre premier. On dit qu'un entier rationnel $a$ est un *résidu quadratique modulo p* si sa classe $\overline{a}$ dans $\mathbf{Z}/p\mathbf{Z}$ y est un carré, i.e. si l'équation $X^2 - \overline{a} = 0$ a une racine dans le corps $\mathbf{F}_p$ (donc deux pour $p \not| a$). Si $p = 2$, tout entier est résidu quadratique modulo 2 (le seul polynôme irréductible de degré 2 de $\mathbf{F}_2[X]$ est $X^2 + X + 1$). C'est aux nombres premiers impairs qu'on s'intéresse donc ici.

Soit $p$ un nombre premier *impair* et $a$ un entier rationnel, de classe $\overline{a}$ modulo $p$ non nulle. On appelle *symbole de Legendre* de $a$ (ou de $\overline{a}$), et on note $(\frac{a}{p})$ (ou $(\frac{\overline{a}}{p})$) le nombre défini par

$$(\tfrac{a}{p}) = 1 \quad \text{si } a \text{ est résidu quadratique modulo } p \ , \ (\tfrac{a}{p}) = -1 \quad \text{sinon} \ .$$

On étend le symbole de Legendre à tous les entiers en posant $(\frac{a}{p}) = 0$ si $p$ divise $a$. Par ailleurs, on identifie les 3 valeurs $\{\pm 1, 0\}$ du symbole de Legendre tantôt à des nombres complexes, tantôt à des éléments du corps $\mathbf{F}_p$ (ou de n'importe quel corps de caract. $\neq 2$).

**Lemme 2**: *i) Pour tout entier a,* $(\frac{a}{p}) = \overline{a}^{\ \frac{p-1}{2}}$*; en particulier,* $(\frac{1}{p}) = 1, (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$*;*
*ii)* $\forall a, b \in \mathbf{Z}, (\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$*, et* $\Sigma_{x \in \mathbf{F_p}} (\frac{x}{p}) = 0$*;*
*iii)* $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

*Démonstration*: i) considérons les endomorphismes $\chi$ et $\psi$ du groupe $\mathbf{F}_p^*$ défini par $\chi(x) = x^{\ \frac{p-1}{2}}, \psi(x) = x^2$. D'après Fermat, $Im\chi \subset Ker\psi = \{\pm 1\}$, et $Im\psi \subset Ker\chi$. Mais $Ker\chi$, formé des éléments d'ordre divisant $(p-1)/2$, coïncide donc avec l'unique sous-groupe d'ordre $(p-1)/2$ du groupe cyclique $\mathbf{F}_p^*$. Idem pour $Im\psi$, d'indice $|Ker\psi| = 2$ dans $\mathbf{F}_p^*$. Finalement, $Ker\chi = Im\psi$, et $(\frac{a}{p}) = 1 \Leftrightarrow \overline{a} \in Im\psi \Leftrightarrow \chi(\overline{a}) = 1$, d'où $(\frac{a}{p}) = \chi(\overline{a})$ pour tout $a$ premier à $p$, soit $(\frac{a}{p}) = \overline{a}^{\ \frac{p-1}{2}}$ pour tout $a$.
ii) La première relation est claire sur $\chi$. Comme $Ker\chi$ est d'indice 2, il y a autant de résidus quadratiques que de non résidus quadr. dans $\mathbf{F}_p^*$, d'où la seconde relation.

iii) Soit $\zeta$ une racine primitive 8-ième de l'unité dans $\overline{\mathbf{F}}_p$. Alors, $\zeta^4 = -1$ et $\theta := \zeta + \zeta^{-1}$ a pour carré 2. On conclut en notant que $(\frac{2}{p}).\theta = \theta^{p-1}\theta = \zeta^p + \zeta^{-p}$ est égal à $\theta$ si $p \equiv \pm 1$ mod 8 , et à $-\theta$ si $p \equiv \pm 3$ mod 8.

*Remarque* 3: soient $G$ un groupe fini. On appelle *caractère* de $G$ tout homomorphisme de groupe de $G$ dans $\mathbf{C}^*$, i.e. toute application $\chi : G \to \mathbf{C}^*$ telle que pour tout $x, y \in G : \chi(xy) = \chi(x)\chi(y)$. En définissant le produit $\chi$ de deux caractères $\chi_1, \chi_2$ par $\chi(x) = \chi_1(x)\chi_2(x)$, on munit l'ensemble $\hat{G}$ des caractères de $G$ d'une structure de groupe, d'élément neutre le caractère trivial $\mathbf{1} : x \mapsto \mathbf{1}(x) := 1$. Avec $\{\pm 1\} \subset \mathbf{C}^*$, le symbole de Legendre devient un caractère du groupe $G = \mathbf{F}_p^*$, d'ordre 2 dans $\hat{G}$, et le lemme 2.ii est un cas particulier des relations générales (exercice):

$$\forall \chi \in \hat{G}, \chi \neq \mathbf{1} : \ \Sigma_{x \in G}\ \chi(x) = 0\ ;\ \Sigma_{x \in G}\ \mathbf{1}(x) = |G|.$$

**Théorème 2** (Gauss): *soient $p$ et $\ell$ deux nombres premiers impairs distincts. Alors*

$$(\frac{\ell}{p})(\frac{p}{\ell}) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}.$$

*Démonstration*: soit $\zeta$ une racine primitive $p$-ième de l'unité dans $\overline{\mathbf{F}}_\ell$, ou dans $\mathbf{C}$. On va calculer de deux façons la "somme de Gauss", bien définie dans chacun de ces corps par la formule

$$S = \sum_{x=0}^{p-1} (\frac{x}{p})\ \zeta^x = \sum\nolimits_{x \in \mathbf{F}_p^*} (\frac{x}{p})\ \zeta^x.$$

(1) *Qu'on lise dans $\overline{\mathbf{F}}_\ell$ ou dans $\mathbf{C}$, on a :* $S^2 = (-1)^{\frac{p-1}{2}} p$.

En effet, $S^2 = \Sigma_{(x,y)}(\frac{xy}{p})\ \zeta^{x+y} = \Sigma_{t \neq 0}(\frac{t}{p})(\Sigma_{x \neq 0}\zeta^{x(1+t)})$, puisque pour $y = xt, (\frac{xy}{p}) = (\frac{x^2}{p})(\frac{t}{p}) = (\frac{t}{p})$. Comme $x \mapsto \zeta^{x(1+t)}$ est un caractère de $(\mathbf{F}_p, +)$, $\Sigma_{x \neq 0}\zeta^{x(1+t)}$ vaut $p-1$ si $p|1+t$, et $-1$ sinon. Ainsi, $S^2 = (\frac{-1}{p})(p-1) + (-1)\Sigma_{t \neq -1}(\frac{t}{p})$, qui vaut $(\frac{-1}{p})p$ d'après le lemme 2, ii).

(2) *Dans $\overline{\mathbf{F}}_\ell$, on a :* $S^{\ell-1} = (\frac{\ell}{p})$.

En effet, comme on est maintenant en caractéristique $\ell$, $S^\ell = \Sigma_x(\frac{x}{p})\ \zeta^{\ell x} = (\frac{\ell}{p})\Sigma_x(\frac{\ell x}{p})\ \zeta^{\ell x} = (\frac{\ell}{p})S$, et on peut diviser par $S$, qui d'après (1), est non nul dans $\overline{\mathbf{F}}_\ell$.

En regroupant (1) et (2), on obtient finalement:

$$(\frac{\ell}{p}) = S^{\ell-1} = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} p^{\frac{\ell-1}{2}} = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} (\frac{p}{\ell}).$$

Cette identité, établie modulo $\ell$, ne relie que des 1 et des -1, et persiste donc en toute caractéristique.

*Remarque* 4: la formule (1), lue en caractéristique 0, montre que pour tout nombre premier $p$ congru à 1 (resp. à 3) modulo 4, l'extension quadratique $\mathbf{Q}(\sqrt{p})$ (resp. $\mathbf{Q}(\sqrt{-p})$ de $\mathbf{Q}$ est contenue dans le corps $\mathbf{Q}(e^{2i\pi/p})$; dans tous les cas, on a donc: $\mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(e^{2i\pi/8p})$. Plus généralement, on déduit de la "théorie du corps de classes" que toute extension abélienne de $\mathbf{Q}$ est contenue dans une extension cyclotomique.

## §3. Factorisation dans $\mathbf{F}_p[X]$. Algorithme de Berlekamp.

Soient $p$ un nombre premier, et $P$ un polynôme unitaire à coefficients dans $\mathbf{Z}$. Comme on l'a dit en I, §2, il suffit, pour que $P$ soit irréductible dans $\mathbf{Q}[X]$, que son image $\pi(P)$ par l'application de réduction modulo $p$ soit irréductible dans $\mathbf{F}_p[X]$. Bien sûr, c'est loin d'être nécessaire: prendre $P(T) = T^2 - \ell$, avec $\ell$ premier, $(\frac{\ell}{p}) = 1$; ou encore: $P(T) = \Phi_{p^d-1}(T)$, irréductible sur $\mathbf{Q}$ d'après la Proposition 3 ci-dessous, bien que tous ses facteurs irréductibles modulo $p$ aient pour degré $d$ (un tel facteur irréductible $\overline{A}$ est le polynôme minimal sur $\mathbf{F}_p$ d'une racine de $\Phi_{p^d-1}$, i.e. d'une racine primitive $p^d - 1$-ième de l'unité dans $\overline{\mathbf{F}}_p$; comme le corps engendré sur $\mathbf{F}_p$ par une telle racine est $\mathbf{F}_{p^d}$, c'est que $deg(\overline{A}) = d$; en particulier, $d|\phi(p^d - 1)$, ce qu'on peut retrouver en notant que $p$ est un élément d'ordre $d$ de $(\mathbf{Z}/(p^d - 1)\mathbf{Z})^*$). Néanmoins, le critère suivant d'irréductibilité sur $\mathbf{F}_p$ s'avère parfois utile.

**Proposition 2**: *Soit $A \in \mathbf{F}_p[X]$ un polynôme de degré $m$. Alors, $A$ est irréductible si et seulement si l'on a simultanément*

$$(X^{p^m} - X, A(X)) = A(X), \text{ et } \forall \ell \text{ premier }, \ell | m : (X^{p^{m/\ell}} - X, A(X)) = 1.$$

*Démonstration*: si $A$ est irréductible, son corps de rupture $\mathbf{F}_p[X]/A(X)\mathbf{F}_p[X] = \mathbf{F}_p(\overline{X})$ sur $\mathbf{F}_p$ a $p^m$ éléments, donc coïncide avec $\mathbf{F}_{p^m}$, et l'itéré de $F$ d'ordre minimal stabilisant $\overline{X}$ est $F^m$. Inversément, tout facteur irréductible de $X^{p^m} - X$ qui ne divise aucun des $X^{p^n} - X$, $n|m, n \neq m$, admet $\mathbf{F}_{p^m}$ pour corps de rupture sur $\mathbf{F}_p$, et est donc de degré $m$.

Voici, à titre d'exercice, un autre type d'application de la réduction modulo $p$ à l'irréductibilité dans $\mathbf{Z}[X]$.

**Proposition 3**: *pour tout entier $n \geq 1$, le polynôme cyclotomique $\Phi_n(X)$ est irréductible dans $\mathbf{Q}[X]$.*

*Démonstration*: soient $\zeta$ une racine primitive $n$-ième de l'unité dans $\overline{\mathbf{Q}}$, et $P$ son polynôme minimal sur $\mathbf{Q}$. D'après le lemme de Gauss (1, §2), on a $\Phi_n = PQ$, avec $P$ et $Q$ unitaires à

coefficients dans $\mathbf{Z}$. On va montrer que toutes les racines primitives $n$-ième de l'unité sont racines de $P$, de sorte que $\Phi_n = P$ est bien irréductible sur $\mathbf{Q}$. Par induction, il suffit de montrer que pour tout nombre premier $p$ ne divisant pas $n$, la racine $\zeta^p$ de $\Phi_n$ est racine de $P$. Sinon, $Q(\zeta^p) = 0$, $\zeta$ est racine du polynôme $R(X) := Q(X^p)$, qui est donc divisible par $P$, et d'après le lemme de Gauss, $\exists S \in \mathbf{Z}[X]$ tel que $R = PS$. D'où par réduction modulo $p$: $\pi(R) = \pi(P)\pi(S)$. Mais $\pi(R(X)) = \pi(Q(X^p)) = \pi(Q(X)^p)$ dans $\mathbf{F}_p[X]$, soit $\pi(P)\pi(S) = (\pi(Q))^p$. Ainsi, tout facteur irréductible $\overline{A}$ de $\pi(P)$ dans $\mathbf{F}_p[X]$ divise $\pi(Q)$, et $\pi(\Phi_n) = \pi(P)\pi(Q)$ est divisible par $\overline{A}^2$. Mais $p \not| n$, donc $\Phi_n$ est un polynôme séparable de $\mathbf{F}_p[X]$, donc sans facteur carré.

Enfin, l'énoncé suivant fournit à la fois un critère d'irréductibilité et un algorithme de factorisation dans $\mathbf{F}_p[X]$.

**Proposition 4** (Berlekamp): *Soit $A \in \mathbf{F}_p[X]$ un polynôme sans facteur carrés, et $A_1...A_r$ sa décomposition en polynômes irréductibles dans $\mathbf{F}_p[X]$. Les polynômes $Q \in \mathbf{F}_p[X]$ nuls ou de degré $< deg(A)$, qui, pour tout $i = 1, ..., r$ , sont congrus modulo $A_i$ à un élément de $\mathbf{F}_p$, sont exactement les $p^r$ polynômes $Q$ nuls ou de degré $< deg(A)$, tels que $Q(X)^p \equiv Q(X)$ $mod(A(X))$.*

*Démonstration*: puisque les $A_i$ sont irréductibles et distincts, ils sont premiers entre eux deux à deux, et le lemme chinois, appliqué à l'anneau principal $\mathbf{F}_p[X]$, permet d'attacher à tout $r$-uplet $(s_1, ..., s_r) \in (\mathbf{F}_p)^r$ de polynômes constants un unique polynôme $Q$ nul ou degré $< deg(A)$ tel que $A_i$ divise $Q - s_i$ pour tout $i$. Alors, $Q^p \equiv s_i^p = s_i \equiv Q \bmod(A_i)$ pour tout $i$, et $A$ divise $Q^p - Q$. Inversément, $X^p - X = \Pi_{s \in \mathbf{F}_p}(X - s)$ dans $\mathbf{F}_p[X]$, donc tout polynôme $Q$ vérifie $Q^p - Q = \Pi_{s \in \mathbf{F}_p}(Q - s)$. Par conséquent, si $A$ divise $Q^p - Q$, chaque facteur irréductible $A_i$ de $A$ divise l'un des facteurs de ce produit, i.e. il existe pour tout $i = 1, ...r$ un polynôme constant $s_i$ tel que $Q \equiv s_i \bmod A_i$. Restreinte aux polynômes $Q$ nuls ou de degré $< deg(A)$, l'application $Q \mapsto (s_1, ..., s_r)$ est la réciproque de la précédente, d'où la bijection recherchée.

*Application*: si $S$ désigne l'endomorphisme $Q \mapsto Q^p$ du $\mathbf{F}_p$-espace vectoriel $\mathbf{F}_p[X]/(A)$ , le noyau de $S - Id$ a pour dimension $\rho = r$, d'où comme promis un critère d'irreductibilité ($\rho = 1$) sur $\mathbf{F}_p$. Et si $\rho \geq 2$, la proposition montre que pour tout élément $Q$ du noyau, il existe $s \in \mathbf{F}_p$ tel que $A$ et $Q - s$ ont un pgcd non trivial, d'où un algorithme de factorisation dans $\mathbf{F}_p[X]$.

# CHAPITRE III

# THÉORIE DE GALOIS

## §1. Extensions galoisiennes.

Soient $K$ un corps et $L/K$ une extension algébrique. On dit que $L/K$ est *normale* si tout élément irréductible de $K[T]$ qui admet une racine dans $L$ se décompose dans $L[T]$ en facteurs linéaires, autrement dit si, pour tout élément $\alpha$ de $L$, il existe des éléments (non nécessairement distincts) $\alpha_1 = \alpha$, $\alpha_2$, .., $\alpha_d$ de $L$ tels que $Min_{\alpha,K}(T) = \Pi_{i=1,...,d}(T - \alpha_i)$; ces racines de $Min_{\alpha,K}$ sont appelées les *conjugués* de $\alpha$ sur $K$ (dans $L$). On dit que $L/K$ est une extension *galoisienne* si elle est à la fois normale et séparable, autrement dit si tout $\alpha \in L$ de degré $d$ sur $K$ admet $d$ conjugués distincts dans $L$. (Rappelons que $L/K$ est dite *séparable* si $\forall \alpha \in L$, le polynôme $Min_{\alpha,K}$ est séparable.)

**Lemme 1**: *i) soit $L/K$ une extension algébrique. Alors, $L/K$ est normale et finie si et slt s'il existe un élément $F$ de $K[T]$ tel que $L$ soit un corps de décomposition de $F$ sur $K$.*

*ii) Soit $L/K$ une extension normale. Pour tout élément $\alpha$ de $L$, l'ensemble des conjugués de $\alpha$ dans $L$ coïncide avec le sous-ensemble de $L$ formé par les images de $\alpha$ sous les différents automorphismes de $L/K$.*

*Démonstration*: i) si $L/K$ est finie, il existe un ensemble fini $S$ d'éléments de $L$ algébriques sur $K$ tels que $L = K(S)$, et si $L/K$ est de plus normale, $F(T) := \Pi_{\alpha \in S} Min_{\alpha,K}(T)$ vérifie la condition demandée.

Inversement, soit $L$ le corps de décomposition d'un élément $F$ de $K[T]$. C'est évidemment une extension finie de $K$. Soient alors $P$ un élément irréductible de $K[T]$ admettant une racine $\alpha$ dans $L$, $N$ un corps de décomposition de $P$ *sur* $L$, et $\alpha'$ une racine quelconque de $P$ dans $N$. Le 1er théorème de prolongement fournit un $K$-isomorphisme $\phi$ de $K(\alpha)$ sur $K(\alpha')$. Puisque $L$ (resp. $L(\alpha')$) est un corps de décomposition de $F$ (resp. $\phi(F)$) sur $K(\alpha)$ (resp. $K(\alpha')$), on déduit du 2ème théorème de prolongement un isomorphisme $\psi$ de $L$ sur $L(\alpha')$ au-dessus de $\phi$. En comparant les degrés, on conclut que $\alpha' \in L$.

ii) Pour tout automorphisme $\sigma$ de $L/K$, $Min_{\alpha,K}(\sigma\alpha) = \sigma(Min_{\alpha,K}(\alpha)) = 0$, et $\sigma\alpha$ est un conjugué de $\alpha$ sur $K$. Inversement, soit $\alpha'$ un conjugué de $\alpha$ sur $K$. Traitons

d'abord le cas où $L/K$ est une extension finie, donc par i), le corps de décomposition d'un $F \in K[T]$. D'après le 1er théorème de prolongement, il existe un $K$-plongement $\phi$ de $K(\alpha)$ dans $L$ envoyant $\alpha$ sur $\alpha'$. D'après le 2e théorème de prolongement, $\phi$ se prolonge en un automorphisme $\sigma$ de $L/K$, et $\sigma(\alpha) = \phi(\alpha) = \alpha'$. D'où la bijection ensembliste annoncée (qui explique qu'on appelle souvent *conjugaisons de* $L/K$ les automorphismes d'une extension normale $L/K$). Le cas général s'en déduit au moyen du lemme de Zorn (considérer l'ensemble des couples $(L', \psi')$ formés d'une extension $L'/K$ normale, contenue dans $L$ et d'un automorphisme $\psi'$ de $L'$ au-dessus de $\phi$, muni de la relation d'ordre $(L_1, \psi_1) < (L_2, \psi_2)$ si $L_1 \subset L_2$ et $\psi_2$ prolonge $\psi_1$.)

Pour toute extension intermédiaire $M/K$ d'une extension normale $L/K$, l'extension $L/M$ est normale (car $\forall \alpha \in L$, $Min_{\alpha,M} | Min_{\alpha,K}$; en revanche, $M/K$ n'est en général pas normale). Par ailleurs, $M/K$ et $L/M$ peuvent être normales sans que $L/K$ le soit. Si $L/K$ est séparable, $M/K$ l'est évidemment, ainsi que $L/M$ (car tout diviseur d'un polynôme séparable est séparable). On verra plus bas que $M/K$ et $L/M$ séparables $\Rightarrow L/K$ séparable.

**Lemme 2** : *Soient $L/K$ une extension* normale, *et $M/K$ une extension intermédiaire.*

*i) Soient $\phi$ un $K$-homomorphisme de $M$ dans $L$, et $\alpha$ un élément de $L$, de degré $d$ sur $M$. Le nombre $d'$ de racines distinctes de $\phi(Min_{\alpha,M})$ dans $L$ vérifie $1 \leq d' \leq d$, et est égal au nombre d'homomorphismes de $M(\alpha)$ dans $L$ au dessus de $\phi$; de plus, $d' = d$ si et seulement si $Min_{\alpha,M}$ est séparable. Plus généralement:*

*ii) Supposons $m = [M : K]$ fini. Le nombre $m'$ de $K$-plongements de $M$ dans $L$ vérifie $1 \leq m' \leq m$, et vaut $m$ si et seulement si $M/K$ est séparable.*

*iii) $M/K$ est normale si et seulement si pour tout $K$-plongement $\phi$ de $M$ dans $L$ , on a: $\phi(M) \subset M$ (et $\phi$ est alors un automorphisme de $M/K$).*

En regroupant les deux dernières conclusions de ce lemme, et en notant $Aut(L/K)$ le groupe des automorphismes d'une extension algébrique $L/K$ (i.e. des automorphismes $\sigma$ du corps $L$ tels que $\forall x \in K, \sigma(x) = x$), on obtient finalement:

**Théorème 1** : *une extension finie $L/K$ est galoisienne si et seulement si le groupe $Aut(L/K)$ est d'ordre $[L : K]$.*

*Démonstration du lemme* 2: i) D'après le 1er théorème de prolongement, le nombre de plongements de $M(\alpha)$ dans $L$ au-dessus de $\phi$ est égal $d'$. De plus, $L/K$ étant normale, $P = Min_{\alpha,K}$ se décompose en facteurs linéaires dans $L$, et il en est de même de $Q = Min_{\alpha,M}$ et de $\phi(Q)$, qui divisent $P = \phi(P)$. En particulier $d' \geq 1$, et $d' = d$ ssi $\phi(Q)$ est séparable sur $K$. Puisque $\phi(Q, DQ) = (\phi(Q), \phi(DQ))$, cela équivaut à demander que $Q$ soit séparable.

ii) récurrence sur $m$. Si $m > 1$, il existe une extension $M_0$ de $K$ et un élément $\alpha$ de $M$ de degré $d > 1$ sur $M_0$ tel que $M = M_0(\alpha)$. Par i), tout $K$-plongement $\phi$ de $M_0$ dans $L$ admet au plus $d$ prolongements $\psi$ à $M$, et exactement $d$ si $M/M_0$, est séparable. Comme tout $K$-plongement $\psi$ de $M$ dans $L$ induit un $\phi$ sur $M_0$, on déduit de l'hypothèse de récurrence qu'il y a $1 \leq m' \leq d[M_0 : K] = m$ $K$-plongements de $M$ dans $L$, et exactement $m$ si $M/K$, donc $M/M_0$ et $M_0/K$, sont séparables.

Supposons maintenant que $M/K$ ne soit pas séparable. Alors, il existe $\alpha \in M$, de degré $d > 1$ sur $K$, non séparable sur $K$, et par i), $d' < d$ $K$-plongements de $K(\alpha)$ dans $L$. On vient de voir que chacun d'eux a au plus $m/d$ prolongements à $M$. Le nombre de $K$-plongements de $M$ dans $L$ est au donc au plus égal à $d'm/d < m$.
[NB: si $M/K$ n'est pas séparable, de sorte que $K$ est de caractéristique $p$ non nulle, on peut en fait démontrer que $m'|m$, et que $\frac{m}{m'}$ est une puissance pure de $p$.]

iii) L'image, par un $K$-plongement $\phi$ de $M$ dans $L$, d'un élément $\alpha$ de $M$ est un conjugué dans $L$ de $\alpha$ sur $K$. Si $M/K$ est normale, ces conjugués sont déjà tous dans $M$, donc $\phi(M) \subset M$, et $\phi$ est un $K$-endomorphisme de $M$. Enfin, *tout endomorphisme $\phi$ d'une extension* algébrique $M/K$ *est un automorphisme*: c'est clair si $[M : K] < \infty$; dans le cas général, remarquer que pour tout $\beta \in M$, l'ensemble $B$ des racines de $Min_{\beta,K}$ dans $M$ est fini, et que $\phi$ induit une injection, donc une bijection, de $B$ sur lui-même; par conséquent, $\beta$ admet dans $B \subset M$ un antécédent sous $\phi$, et $\phi$ est surjectif.

Supposons maintenant que tout $K$-plongement de $M$ dans $L$ laisse stable $M$. Soient $\alpha$ un élément de $M$ et $\alpha'$ un conjugué de $\alpha$ sur $K$. D'après le lemme 1.ii, il existe un automomorphisme $\psi$ de $L/K$ tel que $\psi(\alpha) = \alpha'$. Par hypothèse, la restriction $\phi$ de $\psi$ à $M$ laisse stable $M$, donc $\alpha' = \psi(\alpha) = \phi(\alpha) \in M$. Ainsi, $Min_{\alpha,K}$ se décompose en facteurs linéaires dans $M$, et $M/K$ est normale.
*Preuve du Théorème* 1 : on vient de voir que pour toute extension algébrique, $Aut(L/K)$ coïncide avec l'ensemble des $K$-plongements de $L$ dans $L$. Si $L/K$ est galoisienne finie, il a, d'après le lemme 2.ii, $[L : K]$ éléments. Inversement, soient $L/K$ une extension de degré fini $m = |Aut(L/K)|$, et $\tilde{L}/K$ une extension normale contenant $L$ (par exemple, une clôture algébrique de $L$). Alors, l'ensemble de $K$-plongements de $L$ dans $\tilde{L}$ a au plus $m$ éléments. Comme il contient $Aut(L/K)$, il en a donc $m$ (d'où la séparabilité de $L/K$ grâce au lemme 2.ii), et il coïncide avec ce groupe (d'où la normalité de $L/K$ grâce au lemme 2.iii).

*Remarque* 1: i) soient $L$ une extension normale de $K$ (par exemple, une clôture algébrique de $K$), et $M/K$ une extension intermédiaire. D'après le lemme 2.iii, l'ensemble des extensions normales de $K$ contenant $M$ et contenues dans $L$ admet pour la relation d'inclusion

un plus petit élément $\tilde{M}$ , appelé *clôture normale de $M$ dans $L$*. Si $M/K$ est finie, $\tilde{M}/K$ l'est aussi: en effet, $M = K(S)$, où $S \subset M$ est fini, le polynôme $\Pi_{\alpha \in S} Min_{\alpha,K}$ se décompose en facteurs linéaires dans $L$, et son corps de décomposition $\tilde{M} \subset L$ sur $M$ répond à la question.

ii) On déduit du lemme 2.ii que si $M/K$ et $L/M$ sont deux extensions séparables, alors $L/K$ est séparable. (En considérant les polynômes minimaux, on se ramène au cas où $M/K$ est finie, et $L = M(\alpha)$. Alors, $M$ admet $[M : K]$ $K$-plongements distincts dans $\overline{K}$, et chacun d'eux se prolonge en $[L : M]$ plongements distincts de $L$ dans $\overline{K}$. )

**Lemme 3**: *Toute extension $L/K$ finie et séparable est monogène (i.e. admet un élément $\gamma$, dit primitif pour $L/K$, tel que $L = K(\gamma)$.)*

*Démonstration*: on l'a vérifié au chapitre II quand $K$ est un corps fini. Supposons maintenant $K$ infini. $L/K$ étant de type fini, il suffit par induction de montrer l'assertion quand $L = K(\alpha, \beta)$. Soit $\tilde{L}$ un corps de décomposition de $F = Min_{\alpha,K} Min_{\beta,K}$ sur $L$. D'après le lemme 2.ii, il existe $n = [L : K]$ $K$-plongements distincts $\phi_1, ..., \phi_n$ de $L$ dans $\tilde{L}$. Le polynôme

$$P(T) = \Pi_{1 \leq i \neq j \leq n}[(\phi_i(\alpha) - \phi_j(\alpha)) + (\phi_i(\beta) - \phi_j(\beta))T] \in \tilde{L}[T]$$

est alors non nul; $K$ étant infini, il existe donc $c \in K$ tel que $P(c) \neq 0$, autrement dit tel que les éléments $\phi_i(\alpha + c\beta), i = 1, ..., n$ de $\tilde{L}$ sont distincts. Mais ce sont des racines du polynôme minimal de $\gamma := \alpha + c\beta$ sur $K$, qui est donc de degré $\geq n$. Comme $\gamma \in L$, ce degré est majoré par $n$, et $L = K(\gamma)$.

## §2. La correspondance de Galois.

Soient $L/K$ une extension algébrique, et $G = Aut(L/K)$ le groupe des automorphismes de l'extension $L/K$. Pour toute extension intermédiaire $M$, le groupe $Aut(L/M) = \{\sigma \in G; \forall x \in M, \sigma(x) = x\}$ des automorphismes de l'extension $L/M$ est un sous-groupe de $G$. Inversement, pour tout sous-groupe $H$ de $G$, le corps $L^H := \{x \in L; \forall \sigma \in H, \sigma(x) = x\}$ est une extension intermédiaire de l'extension $L/K$, appelé *sous-corps de $L$ fixé par $H$*. On a:

$$H < H' < G \Rightarrow K \subset L^{H'} \subset L^H \subset L \quad ;$$
$$K \subset M \subset M' \subset L \Rightarrow Aut(L/M') < Aut(L/M) < G.$$

Toute extension intermédiaire $M$ est contenue dans $L^{Aut(L/M)}$, mais il se peut qu'elle le soit strictement (exemple: $K = M = \mathbf{Q} \subset L = \mathbf{Q}(\sqrt[3]{2})$, pour lequel $Aut(L/K) = \{id_L\}$, $L^{Aut(L/K)} = L$). De même, tout sous-groupe $H$ de $G$ est contenu dans $Aut(L/L^H)$, mais

peut l'être strictement (exemple hors programme: $K = \mathbf{F}_p \subset L = \overline{K}, H = \{F^n, n \in \mathbf{Z}\}$, où $F$ désigne le Frobenius de $L$; alors $L^H = K$, mais $Aut(L/K)$ est bien plus gros que $H$). Pour simplifier l'exposé, nous nous limiterons pour l'essentiel aux groupes finis, où ce deuxième type de contre-exemples n'apparaît pas. Quant au premier type de contre-exemples, il disparaît lorsqu'on se restreint à des extensions $L/K$ *galoisiennes*.

Pour $L/K$ galoisienne, le groupe $Aut(L/K)$ s'appelle le *groupe de Galois de l'extension galoisienne* $L/K$, et est souvent noté $Gal(L/K)$.

**Théorème 2**: *i) Soient $L/k$ une extension quelconque, $G$ un sous-groupe* fini *de $Aut(L/k)$, et $K$ le corps $L^G$. Alors, $L/K$ est une extension galoisienne finie, et $Aut(L/K) = G$.*

*ii) Soient $L/k$ une extension* algébrique, *$G$ un sous-groupe quelconque de $Aut(L/k)$, et $K$ le corps $L^G$. Alors, $L/K$ est une extension galoisienne*

*iii) Soit $L/K$ une extension galoisienne. Alors, $L^{Aut(L/K)} = K$.*

On obtient ainsi une nouveau critère pour qu'une extension algébrique $L/K$, finie ou non, soit galoisienne: il faut et il suffit que $L^{Aut(L/K)} = K$.

*Démonstration*: i) Soient $\alpha$ un élément de $L$, et $\sigma_1 = \mathrm{id}_L, \sigma_2, ...\sigma_r$ un sous-ensemble *maximal* de $G$ tel que $\sigma_1\alpha, ..., \sigma_r\alpha$ soient distincts. Posons $P(T) = \Pi_{i=1,...r}(T - \sigma_i\alpha) \in L[T]$. Alors, $\sigma(P) = P$ pour tout $\sigma \in G$, de sorte que $P \in K[T]$, et $\alpha$ est algébrique sur $K$. De plus, $Min_{\alpha,K}$ divise $P$, mais est aussi divisible par $P$ puisque $Min_{\alpha,K}(\sigma_i\alpha) = \sigma_i(Min_{\alpha,K}(\alpha)) = 0$; bref, $Min_{\alpha,K} = P$. Ainsi, le polynôme minimal de $\alpha$ sur $K$ se décompose en facteurs linéaires distincts dans $L$, et $L/K$ est galoisienne.

On vient de montrer que le polynôme minimal sur $K$ de tout élément de $L$ est de degré $\leq |G|$, i.e. que tous les éléments de $L$ sont de degé $\leq |G|$ sur $K$. Comme $L/K$ est séparable, il résulte alors du lemme 3 que $[L : K] \leq |G|$. Enfin, $[L : K] = |Aut(L/K)|$ d'après le théorème 1, et $G$ est un sous-groupe de $Aut(L/L^G)$. Par conséquent, $L/K$ est degré $\geq |G|$, donc finalement égal à $|G|$, et $G$ remplit tout $Aut(L/K)$.

ii) Si $L/k$ est algébrique, l'orbite sous $G$, éventuellement infini, de tout élément $\alpha$ de $L$ est formée de racines de $Min_{\alpha,k}$, et est donc finie. La première partie du raisonnement de i) reste donc valable, et $L/K$ est galoisienne.

iii) Soit $\alpha$ un élément de $L$, de degré $d$ sur $K$. D'après les lemmes 2.i et 1.ii, il existe $d$ automorphismes $\sigma_1 = \mathrm{id}, ..., \sigma_d$ de $L/K$ tels que $\{\sigma_i\alpha; i = 1, ...d\}$ forme l'ensemble des racines de $Min_{\alpha,K}$ dans $L$. Si maintenant $\alpha \in K^G$, on a $\sigma_i(\alpha) = \alpha$ pour tout $i = 1, ..., d$, et $d = 1$. Ainsi, $\alpha$ appartient à $K$, et $K^G = K$.

*Remarque* 3: pour démontrer l'inégalité $[L : K] \geq |G|$ au théorème 2.i, on peut également procéder de la manière suivante. Voyons $G \subset Aut(L/K)$ comme une famille d'éléments du

$L$-espace vectoriel $F(\Gamma, L)$ des fonctions sur $\Gamma := L^*$, à valeurs dans $L$. Si $[L : K] < |G|$, elle est linéairement dépendante sur $L$. Mais les éléments de $G$ sont aussi des caractères du groupe $\Gamma$ (à valeurs dans le groupe multiplicatif du corps $L$), et un théorème classique, valable pour tout groupe $\Gamma$ et tout corps $L$, affirme que des caractères distincts de $\Gamma$ forment une famille $L$-libre dans $F(\Gamma, L)$.

**Théorème de Galois**: *soient $L/K$ une extension galoisienne finie, et $G = Gal(L/K)$ son groupe de Galois.*

*i) Soit $M$ un extension intermédiaire, et $H = Gal(L/M) < G$ le groupe de Galois de l'extension (galoisienne) $L/M$; alors, $[L : M] = |H|$, et $M = L^H$;*

*ii) Soit $H$ un sous-groupe de $G$, et $M = L^H$ le sous-corps de $L$ fixé par $H$; alors $L/M$ est une extension galoisienne de degré $[L : M] = |H|$, et $H = Gal(L/M)$;*

*iii) Une extension intermédiaire $M/K$ est galoisienne si et seulement si $H := Gal(L/M)$ est un sous-groupe distingué de $G$; dans ce cas, son groupe de Galois $Gal(M/K)$ s'identifie au groupe quotient $G/H$.*

*Démonstration*: i) et ii) sont des réécritures du théorème 2. (Mais en ii), le fait que $L/L^H$ est galoisienne n'est pas profond, puisqu'on part d'une extension $L/K$ galoisienne.) Passons à iii).

Supposons $M/K$ galoisienne, et soient $\tau \in G, \sigma \in H$. Il s'agit de voir que $\tau^{-1}\sigma\tau$ appartient à $H$, i.e. fixe chaque élément $x$ de $M$. Comme $\tau(x)$ est une racine de $Min_{x,M}$ et que $M/K$ est normale, $\tau(x) \in M$, et est donc fixé par $\sigma$. Alors, $\tau^{-1}\sigma\tau(x) = \tau^{-1}\tau(x) = x$.

Supposons $H$ distingué dans $G$. Il s'agit de voir que $M/K$ est normale (comme $L/K$ est séparable, on sait déjà que $M/K$ l'est aussi). Les conjugués dans $L$ d'un élément $x \in M$ sont de la forme $\tau(x), \tau \in G$. Mais pour tout $\sigma \in H, \tau^{-1}\sigma\tau := \sigma'$ appartient à $H \lhd G$, donc fixe $x$, et $\sigma\tau(x) = \tau\sigma'(x) = \tau(x)$, soit $\tau(x) \in L^H = M$.

Dans ces conditions, tout automorphisme $\sigma$ de $L/K$ induit sur $M$ un automorphisme $\sigma_{|M}$ de $M$ (cf. lemme 2.iii), de sorte que l'application $\pi : \sigma \mapsto \sigma_{|M}$ définit un homomorphisme de groupe de $G$ dans $Gal(M/K)$. Mais $\pi$ est surjective d'après le deuxième théorème de prolongement, et son noyau est formé des automorphismes de $L/K$ induisant l'identité sur $M$. Autrement dit, $Ker(\pi) = Gal(L/M)$, et $Gal(M/K) \simeq G/H$.

Le théorème de Galois montre que l'étude des extensions intermédiaires d'une extension galoisienne finie $L/K$ équivaut à celle des sous-groupes de $Gal(L/K)$. Par exemple, on en déduit immédiatement que $L/K$ n'a qu'un nombre fini d'extensions intermédiaires (cela reste vrai si $L/K$ est seulement séparable, sinon, c'est en général faux). De ce fait, on désigne souvent du même adjectif les propriétés d'une extension galoisienne et celles de

leurs groupes de Galois. Ainsi, une extension galoisienne est dite abélienne (resp. cyclique) si son groupe de Galois l'est. Dans l'autre sens, on voit pourquoi 'normal' et 'distingué' sont synonymes en théorie des groupes; quant au mot 'résoluble', il fait l'objet du §3.

## §3. Applications

Pour alléger l'exposé, nous présentons ces applications sous forme de séries d'exercices, et nous nous plaçons en caractéristique nulle (toutes les extensions sont donc séparables).

*a) Resolubilite par radicaux*

Soit $K$ un corps (de caractéristique nulle). Une extension $M/K$ est dite *résoluble* s'il existe une tour d'extensions $K = K_0 \subset K_1 \subset ... \subset K_m = M$ telle que pour tout $i = 1, ..., m$, il existe un élément $\beta_i$ de $K_i$ et un entier $n_i > 0$ tel que $\beta_i^{n_i} \in K_{i-1}$ et $K_i = K_{i-1}(\beta_i)$. Pour $F \in K[T]$, de corps de décomposition $K_F$ sur $K$, on dit que l'équation $F(x) = 0$ est *résoluble par radicaux* si l'extension $K_F/K$ est contenue dans une extension résoluble de $K$. Par ailleurs, on appelle souvent *groupe de Galois de* $F$ le groupe $Gal(K_F/K)$.

Dans le problème étudié ici, on peut se ramener au cas où $K$ contient pour tout entier $n > 0$ une racine primitive $n$-ième de l'unité. C'est ce que nous supposerons désormais. Si $M/K$ est résoluble, chacune des extensions intermédiaires $K_i/K_{i-1}$ est alors galoisienne, de groupe de Galois isomorphe à un sous-groupe de $\mathbf{Z}/n_i\mathbf{Z}$, donc abélien (et même cyclique). Inversement, on peut démontrer, au moyen du "théorème 90 de Hilbert", que toute extension cyclique $K''/K'$, de degré $n$, d'un corps $K'$ contenant une racine primitive $n$-ième de l'unité, est de la forme $K'' = K'(\beta^{\frac{1}{n}})$, où $\beta \in K'$.
*Ex. 1*: soit $M/K$ une extension résoluble, et $N/K$ une clôture normale de $M/K$. Alors, $N/K$ est une extension résoluble.

Soit $G$ un groupe. On dit que $G$ est *résoluble* s'il admet une suite de sous-groupes $G_m = \{e\} < G_{m-1} < ... < G_1 < G_0 = G$ telle que pour tout $i = 1, ..., m$, $G_i$ soit distingué dans $G_{i-1}$ et $G_{i-1}/G_i$ soit abélien.

On démontre en théorie des groupes que si $G$ est un groupe résoluble, et si $H \triangleleft G$, alors $G/H$ est résoluble.

*Ex. 2*: Soit $M/K$ une extension résoluble , et $L/K$ une extension intermédiaire. Alors, $Aut(L/K)$ est un groupe résoluble.
[Noter que si $K' = L^{Aut(L/K)}$, $M/K'$ est résoluble, et $L/K'$ est galoisienne, de groupe de Galois $Aut(L/K') = Aut(L/K)$. Par l'ex. 1 et la remarque précédente sur $G/H$, il suffit alors de montrer que si $N/K$ est galoisienne et résoluble, le groupe $Gal(N/K)$ est résoluble.]

On obtient en définitive:

**Théorème A**: *une équation $F(x) = 0$ à coefficients dans $K$ est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

*b) L'équation générale de degré n.*

Soient $k$ un corps de caractéristique 0, et $\mathbf{K} = k(u_1, ..., u_n)$ le corps des fractions rationnelles en $n$ variables. *L'equation générale de degré n* est l'équation $\mathbf{P}_n(x) = 0$, où $\mathbf{P}_n(T) = T^n - u_1 T^{n-1} + ... + (-1)^n u_n \in \mathbf{K}[T]$. Soit $\mathbf{L} = \mathbf{K}(v_1, ..., v_n)$ le corps de décomposition de $\mathbf{P}_n$ sur $\mathbf{K}$, avec $\mathbf{P}_n(T) = \Pi_{i=1,...,n}(T - v_i)$. On a: $u_1 = v_1 + ... + v_n$, $u_2 = \Sigma_{1 \leq i < j \leq n} v_i v_j$, ... , $u_n = \Pi_{i=1,...,n} v_i$.

Soit par ailleurs $L = k(x_1, ..., x_n)$ le corps des fractions rationnelles en $n$ nouvelles variables $x_1, ..., x_n$. L'action du groupe symétrique $S_n$ sur $L$, définie, pour tout $f \in L$, par $(\sigma f)(x_1, ..., x_n) := f(x_{\sigma(1)}, ..., x_{\sigma(n)})$, identifie $S_n$ à un sous-groupe de $Aut(L/k)$. Les élements du corps $S = L^{S_n}$ sont appelés les *fonctions symétriques* en les $x_i$. Soit $K := k(s_1, ..., s_n)$ le sous-corps de $S$ engendré par les fonctions symétriques *élémentaires* $s_1 = x_1 + ... + x_n$, $s_2 = \Sigma_{1 \leq i < j \leq n} x_i x_j$, ... , $s_n = \Pi_{i=1,...,n} x_i$.

**Théorème B'**: *toute fonction symétrique s'exprime comme une fraction rationelle en les fonctions symétriques élémentaires. Autrement dit, on a $K = S$ (et $Aut(L/K) = S_n$).*
[D'après le thm. 3.i, $[L : S] = |S_n| = n!$, donc $[L : K] \geq n!$. Pour l'inégalité inverse, noter que pour tout corps $K'$, le corps de décomposition sur $K'$ de tout élément de $K'[T]$ de degré $n$ est de degré au plus $n!$. Considérer alors $P_n(T) = T^n - s_1 T^{n-1} + ... + (-1)^n s_n \in K[T]$.]

On peut montrer que l'homomorphisme d'anneaux $ev : k[u_1, ..., u_n] \to K : P \mapsto P(s_1, ..., s_n)$ est injectif. Il s'etend donc en un isomorphisme $\phi$ de $\mathbf{K}$ sur $K$.
*Ex. 3*: les extensions $\mathbf{L}/\mathbf{K}$ et $L/K$ sont isomorphes. En particulier, *l'équation générale de degré n admet $S_n$ pour groupe de Galois.*

Or on démontre en théorie des groupes que $S_n$ est un groupe résoluble si $n \leq 4$, et non résoluble dès que $n \geq 5$. Du théorème A, on déduit donc:

**Théorème B**: *l'équation générale de degré n est résoluble par radicaux si et slt si $n \leq 4$.*

Reste à trouver les formules par radicaux donnant les solutions de ces équations. Expliquons la méthode pour $n = 3$ (formule de Cardan). On suppose comme toujours que $car(k) = 0$, et pour simplifier, que $k$ contient les racines cubiques $\rho, \rho^2$ de l'unité. On met sans difficulté $\mathbf{P}_3$ sous la forme $\mathcal{P}(T) = T^3 + pT + q = (T - v_1)(T - v_2)(T - v_3)$, de discriminant $D = -4p^3 - 27q^2$, qui n'est pas un carré dans le corps de base $\mathcal{K} = k(p, q)$. Le sous-corps de $\mathcal{L} = \mathcal{K}(v_1, v_2, v_3)$ fixé par le groupe alterné $A_3$, d'indice 2 dans $S_3 =$

$Gal(\mathcal{L}/\mathcal{K})$, est l'extension quadratique $\mathcal{K}(\sqrt{D})$, avec $\sqrt{D} = (v_1 - v_2)(v_2 - v_3)(v_3 - v_1)$. Considérons alors les éléments $\eta = v_1 + \rho v_2 + \rho^2 v_3$, $\zeta = v_1 + \rho^2 v_2 + \rho v_3$ de $\mathcal{L}$. Leurs cubes sont invariants sous $A_3$, donc appartiennent à $\mathcal{K}(\sqrt{D})$. On vérifie en explicitant le théorème B (formules de Newton, avec $v_1 + v_2 + v_3 = 0$) que

$$\eta^3 = \frac{1}{2}(-27q + 3\sqrt{-3}\sqrt{D}) \ , \ \zeta^3 = \frac{1}{2}(-27q - 3\sqrt{-3}\sqrt{D}),$$

où $\sqrt{-3} = \rho - \rho^2$. De plus, $\eta\zeta$ est invariant sous $S_3$, donc appartient à $\mathcal{K}$ (le calcul donne $\eta\zeta = -3p$). Ainsi,

$$v_1 = \frac{1}{3}(\eta + \zeta), \ v_2 = \frac{1}{3}(\rho^2\eta + \rho\zeta) \ , v_3 = \frac{1}{3}(\rho\eta + \rho^2\zeta).$$

La condition sur $\eta\zeta$ assure qu'on obtient ainsi, à permutation paire près, un unique triplet de solutions de $\mathcal{P}(x) = 0$.

*c) Constructions à la règle et au compas*

Soient $S$ (resp. $P$) une collection finie de points (resp. un point) du plan, et $K$ (resp. $K(P)$) le corps engendré par les coordonnées des points de $S$ (resp. l'extension de $K$ engendrée par celles de $P$) dans un repère orthonormé. 0n suppose que l'origine et le point $(0, 1)$ appartiennent à $S$. Comme l'équation aux abscisses des points d'intersection d'une droite ou d'un cercle avec une droite ou un cercle est au plus quadratique, dire que $P$ est constructible à la règle et au compas à partir de $S$ équivaut à dire qu'il existe une tour d'extensions $K_0 = K \subset K_1 \subset ... \subset K_m$ telle que pour tout $i = 1, ..., m$, $K_i/K_{i-1}$ soit une extension quadratique et que $K_m$ contienne $K(P)$.

*Ex. 4*: avec les notations ci-dessus, soit $N/K$ une clôture normale de $K_m/K$. Montrer que $[N : K]$ est une puissance de 2.

Soient $p$ un nombre premier, et $G$ un groupe fini. On dit que $G$ est un $p$-groupe si son ordre est une puissance de $p$. On montre en théorie des groupes que tout $p$-groupe est résoluble. En considérant les extensions intermédaires attachées à la suite de sous-groupes correspondants, on en déduit:

**Théorème C** : *$P$ est constructible à la règle et au compas à partir de $S$ si et seulement s'il existe une extension $N$ de $K(P)$, galoisienne sur $K$, telle que $Gal(N/K)$ soit un 2-groupe.*

On appelle nombre premier de Fermat tout nombre premier de la forme $2^{2^n} + 1$, où $n \geq 0$. On n'en connait pour l'instant que 5 ($n = 0, 1, 2, 3, 4$).

*Ex. 5*: Soit $N$ un entier $\geq 1$. On considère dans le plan complexe l'ensemble $S = \{0, 1\}$, et le point $P_N = exp(2i\pi/N)$. Montrer que $P_N$ est constructible à la règle et au compas

à partir de $S$ si et seulement si $N$ est le produit d'une puissance de 2 par un produit de nombres premiers de Fermat distincts.
[Indication: utiliser II, Proposition 3.] On laisse au lecteur le soin de découper une pizza (à la règle et au compas) en 65 537 parties égales.