Cours de théorie des corps

Marc Reversat et Benoît Zhang
Université Paul Sabatier de Toulouse
reversat@picard.ups-tlse.fr, zhang@picard.ups-tlse.fr

24 mars 2003

Prologue

L'objet de ce cours est l'étude des équations d'une variable[1]. Étant donnés un corps K et $P(X)$ un polynôme à coefficients dans K, on s'intéresse aux solutions (éventuellement dans un corps plus gros) de l'équation

$$(*) \qquad P(X) = 0.$$

L'exemple le plus important est lorsque $K = \mathbb{Q}$, auquel cas on cherche les solutions dans $\mathbb{C}$.

En exposant la Théorie de Galois on montre comment à une telle équation se trouve associé un groupe, le Groupe de Galois d'un corps de décomposition de $P(X)$ sur K, les propriétés de ce groupe donnant beaucoup d'informations sur celles de l'équation. Au chapitre 7 on s'intéresse aussi à l'idée naturelle, étant donné une équation à coefficients entiers, consistant à la réduire modulo les nombres premiers p, elle devient alors à coefficients dans les corps finis $\mathbb{Z}/p\mathbb{Z}$, une situation dont on verra qu'elle est plus simple, mais qui nécessite nombre de résultats "d'algèbre abstraite" (objets de nombreux travaux des arithméticiens de la fin du 19-ème siècle et du début du 20-ème) afin d'exploiter les informations supplémentaires ainsi obtenues.

Une autre idée naturelle vient peut-être à l'esprit, la question inverse de celle résolue par la Théorie de Galois : étant donné un groupe (fini), est-il le Groupe de Galois d'une équation $(*)$? Lorsque les coefficients de $P(X)$ sont dans $\mathbb{Q}$, c'est un problème crucial de l'arithmétique, qui est loin d'être résolu aujourd'hui, nous n'en dirons donc rien, sauf peut-être par notre insistance à énoncer des résultats valables en toutes caractéristiques. En effet, le même problème, avec par exemple le corps des fractions rationnelles $\mathbb{F}(T)$ (où $\mathbb{F}$ est un corps fini) pour corps des coefficients, vient d'être presque résolu[2], et cette situation est un bon modèle pour certains aspects de la question sur le corps $\mathbb{Q}$.

[1] Ce polycopié s'appuie sur une première version du cours rédigée par Françoise et Bruno Grébille.

[2] Par Laurent Lafforgue, 2002.

Table des matières

Prologue **iii**

1 Généralités **1**
1.1 Extensions de corps 1
1.2 Caractéristique d'un corps 4
1.3 Extensions algébriques 5
1.4 Corps de ruptures 8
1.5 Clôtures algébriques 9
1.6 Exercices 15

2 Corps de décomposition, extensions normales **19**
2.1 Corps de décompositions 19
2.2 Extensions normales 21
2.3 Fermetures normales 22
2.4 Exercices 24

3 Séparabilité et inséparabilité **27**
3.1 Le degré de séparabilité 27
3.2 Les extensions séparables 30
3.3 Les extensions purement inséparables 34
3.4 Séparabilité et normalité 35
3.5 Les corps parfaits 36
3.6 Les extensions monogènes 37
3.7 La norme et la trace 39
3.8 Exercices 45

4 Théorie de Galois **49**
4.1 La correspondance de Galois 49
4.2 Compléments 51
4.3 Le théorème de la base normale 53
4.4 Exercices 56

5 Exemples d'extensions galoisiennes 59
5.1 Les extensions cyclotomiques 59
5.2 Les corps finis 62
5.3 Sur les extensions cycliques 66
5.4 Une clôture algébrique de $\mathbb{R}$ 68
5.5 Exercices 70

6 Les équations résolubles par radicaux 73
6.1 A propos des équations de degrés 2 à 5 73
6.1.1 Le degré 2 73
6.1.2 Le degré 3 73
6.1.3 Le degré 4 75
6.1.4 Une équation de degré 5 76
6.1.5 Conclusion 77
6.2 Les extensions résolubles 78
6.3 Exercices 84

7 A la recherche d'informations sur quelques groupes de Galois 89
7.1 Les modules 89
7.1.1 Généralités 89
7.1.2 Quotients 90
7.1.3 Modules noethériens 91
7.2 Intégralité 92
7.2.1 Éléments entiers sur un anneau 92
7.2.2 Quelques propriétés des anneaux intégralement clos . . 94
7.2.3 Sur quelques fermetures intégrales 95
7.3 Idéaux premiers 97
7.3.1 Les anneaux de fractions 97
7.3.2 A propos des modules de type fini 98
7.3.3 Prolongements des idéaux premiers 99
7.3.4 Le cas des extensions algébriques 99
7.4 Idéaux premiers et extensions galoisiennes 101
7.4.1 Groupes de décomposition 101
7.4.2 Applications 103
7.5 Exercices 105

8 Appendice : Les anneaux factoriels 107
8.1 Généralités 107
8.2 Anneaux principaux et anneaux factoriels 110
8.3 Anneaux factoriels et polynômes 111
8.4 Anneaux factoriels et anneaux de fractions 114
8.5 Exercices 116

9 Exercices complémentaires **119**

Index **132**

Chapitre 1

Généralités

On rappelle qu'un corps K est un anneau unitaire avec $1_K \neq 0$, pour des opérations que l'on notera toujours additivement et multiplicativement, dans lequel tout élément non nul est inversible pour la multiplication. Il suit que tous les idéaux de K sont triviaux, i.e. égaux à $\{0\}$ ou à K. Les morphismes de corps $\varphi : K \to L$ sont les morphismes d'anneaux entre deux corps. Il résulte de la nature des idéaux d'un corps qu'un tel morphisme est ou bien nul ($\varphi(x) = 0$ pour tout x de K), ou bien injectif. Dans tout ce cours on suppose que les morphismes de corps $\varphi : K \to L$ sont unitaires, c'est à dire qu'ils envoient l'élément unité de K sur celui de L, par suite *ils seront tous injectifs.*

Sauf mention expresse du contraire, *tous les anneaux et les corps sont supposés commutatifs.*

1.1 Extensions de corps

Définition 1.1.1. Soit L un corps et K un sous-corps de L. On dit alors que L est une extension de K, et l'on écrit L/K (qui se lit "L sur K"). Soit E/K une extension et L un corps intermédiaire entre E et K (donc $K \subseteq L \subseteq E$ et ces inclusions sont entre corps et sous-corps), on dit alors que L/K et E/L sont des sous-extensions de E/K.

Remarque 1.1.2. On se gardera bien de confondre inclusions et injections, même canoniques. Par exemple, $E = \mathbb{Q}[X]/(X^2 - 2)$ est un corps muni d'une injection canonique $E \hookrightarrow \mathbb{R}$ venant de l'application $\mathbb{Q}[X] \to \mathbb{R}$ qui à X associe $\sqrt{2}$. De même, étant donné une autre indéterminée Y, on a une injection canonique $F = \mathbb{Q}[Y]/(Y^2 - 2) \hookrightarrow \mathbb{R}$. Les corps E et F sont distincts, mais si l'on confond ces injections canoniques avec des inclusions, ils deviennent égaux (il faut bien que le polynôme $X^2 - 2$ n'ait pas plus de deux racines dans $\mathbb{R}$) !

Définition 1.1.3. Soient L/K et E/K deux extensions du corps K. Un morphisme de corps : $L \to E$ trivial sur K est appelé un K-homomorphisme ou un K-morphisme. L'ensemble des K-homomorphismes de L dans E est noté $\mathrm{Hom}_K(L, E)$. Lorsque $L = E$ on parle de K-endomorphismes et l'on écrit $\mathrm{End}_K(L)$, ou encore $\mathrm{Aut}_K(L)$ lorsque l'on ne considère que les automorphismes (les K-automorphismes), ce dernier ensemble étant un groupe pour la composition des applications.

Définition 1.1.4. Soit L/K une extension, alors les opérations dont L est muni en font un K-espace vectoriel. On dit que l'extension L/K est finie si L est un K-espace vectoriel de dimension finie. La dimension de L sur K se note $[L : K]$ et s'appelle le degré de L sur K, ou encore le degré de l'extension L/K. Les K-bases de L sont aussi appelées bases de l'extension L/K.

Proposition 1.1.5. *Soient L/K et E/L deux extensions (donc on a $K \subseteq L \subseteq E$ et ces inclusions sont entre corps et sous-corps), les assertions suivantes sont équivalentes :*
(i) E/K est une extension finie,
(ii) les extensions L/K et E/L sont finies.
Si l'une de ces assertions est vraie, on a de plus la formule suivante

$$[E : K] = [E : L][L : K].$$

Démonstration. Si (i) est vraie. Le corps L est un sous-K-espace vectoriel de E et tout système générateur de E sur K l'est à plus forte raison sur L.

Si (ii) est vraie. Soient $\{u_i\}_{1\leq i\leq r}$ une base de L/K et $\{v_i\}_{1\leq i\leq s}$ une base de E/L. Alors

$$\{u_i v_j\}_{1\leq i\leq r, 1\leq j\leq s}$$

est une base de E/K. En effet :
- C'est un système générateur. Soit $x \in L$, alors x s'écrit $x = \sum_{1\leq j\leq s} \lambda_j v_j$ avec les λ_j dans L, qui donc s'écrivent sous la forme $\lambda_j = \sum_{1\leq i\leq r} \mu_{i,j} u_i$ où les $\mu_{i,j}$ sont dans K. On a donc

$$x = \sum_{1\leq i\leq r, 1\leq j\leq s} \mu_{i,j} u_i v_j.$$

- C'est une partie libre. Soit

$$\sum_{1\leq i\leq r, 1\leq j\leq s} \mu_{i,j} u_i v_j = 0 \text{ avec les } \mu_{i,j} \text{ dans } K.$$

Il vient

$$0 = \sum_{1\leq i\leq r, 1\leq j\leq s} \mu_{i,j} u_i v_j = \sum_{1\leq j\leq s} \Big(\sum_{1\leq i\leq r} \mu_{i,j} u_i \Big) v_j,$$

donc, puisque $\{v_i\}_{1\leq i\leq s}$ est libre sur L

$$\sum_{1\leq i\leq r} \mu_{i,j}u_i = 0 \text{ pour } 1 \leq j \leq s,$$

dont on déduit que les $\mu_{i,j}$ sont tous nuls, puisque $\{u_i\}_{1\leq i\leq r}$ est libre sur K. □

Soient L/K une extension et M une partie de L, alors il existe un plus petit sous-corps de L contenant K et M, c'est l'intersection de tous les sous-corps de L contenant K et M.

Définition 1.1.6. Soient L/K une extension et M une partie de L. Le plus petit sous-corps de L contenant K et M s'appelle le sous-corps de L engendré sur K par M, ou encore la sous-extension de L/K engendrée par M. Ce corps se note $K(M)$, ou $K(x_1, \cdots, x_r)$ si M est fini, $M = \{x_1, \cdots, x_r\}$.

Proposition 1.1.7. *Soient L/K une extension et M une partie de L. Alors $K(M)$ est l'ensemble des expressions de la forme $P(x_1, \cdots, x_n)/Q(x_1, \cdots, x_n)$ où $x_1, \cdots, x_n \in M$, $n \in \mathbb{N}$, $n \leq$ card(M), où $P, Q \in K[X_1, \cdots, X_n]$ sont des polynômes avec $Q(x_1, \cdots, x_n) \neq 0$.*

Démonstration. Les lois de corps impliquent que ces éléments sont dans $K(M)$ et il est facile de vérifier que leur ensemble contient K, contient M et forme un corps pour les lois de L. □

Remarque 1.1.8. Soient L/K une extension et M une partie de L. Il ne faut pas confondre $K(M)$ et $K[M]$, le deuxième étant le sous-anneau engendré par K et M. Rappelons que cet anneau $K[M]$ est l'ensemble des expressions polynomiales de la forme $P(x_1, \cdots, x_n)$ où $x_1, \cdots, x_n \in M$, $n \in \mathbb{N}$, $n \leq$ card(M), où $P \in K[X_1, \cdots, X_n]$ est un polynôme. En général on a $K[M] \neq K(M)$, par exemple si $M = \{X\}$, où X est une indéterminée, l'anneau des polynômes $K[X]$ n'est pas égal au corps des fractions rationnelles $K(X)$. Cependant il y a égalité pour une classe d'extensions de corps, les extensions algébriques, qui sont l'objet d'étude principal ici et qui seront définies au §1.3. En guise de préliminaire, on pourra montrer que par exemple que l'anneau $\mathbb{Q}[\sqrt{2}]$ est égal au corps $\mathbb{Q}(\sqrt{2})$. Une autre remarque intéressante est de constater que le corps des fractions de $K[M]$ est $K(M)$.

Proposition 1.1.9. *Soit L/K une extension.*
(i) Soit M et N deux parties de L, alors on a

$$K(M \cup N) = K(M)(N) = K(N)(M).$$

(ii) Soit M une partie de L, alors on a

$$K(M) = \bigcup_{F\subset M, F\, fini} K(F).$$

Démonstration. Ces assertions sont faciles, par exemple, pour la première : On a K et M dans $K(M \cup N)$, donc $K(M) \subset K(M \cup N)$ et puisque N est aussi dans $K(M \cup N)$, il vient $K(M)(N) \subset K(M \cup N)$. Réciproquement, $M \cup N$ et K sont dans $K(M)(N)$, d'où l'inclusion inverse. Etc. □

Cette dernière proposition permet la définition suivante

Définition 1.1.10. Soient K_1 et K_2 deux sous-corps d'un même troisième L. On appelle compositum de K_1 et K_2 le corps $K_1(K_2) = K_2(K_1)$, que l'on note $K_1 \cdot K_2$.

Parler du compositum de deux corps non inclus dans un même troisième n'a pas de sens, pour s'en convaincre, on peut par exemple examiner les deux corps E et F de la remarque 1.1.2.

Définition 1.1.11. Soit L/K une extension. On dit que c'est une extension de type fini s'il existe une partie finie M de L telle que $L = K(M)$.

Remarque 1.1.12. Une extension L/K finie est de type fini, en effet, si $\{u_1, \cdots, u_n\}$ est une K-base de L, on a $L = K(u_1, \cdots, u_n)$. La réciproque est fausse, par exemple, le corps des fractions rationnelles $K(X)$ est une extension de type fini de K mais n'est pas une extension finie de K.

1.2 Caractéristique d'un corps

Soient K un corps et $\varphi_K : \mathbb{Z} \to K$ le morphisme qui à l'entier n associe $n1_K \in K$, où 1_K est l'élément unitaire de K. Comme K est intègre, le noyau de φ_K est un idéal premier de $\mathbb{Z}$, c'est à dire que l'on a $\mathrm{Ker}\varphi_K = \{0\}$ ou $\mathrm{Ker}\varphi_K = p\mathbb{Z}$, p étant un nombre premier.

Définition 1.2.1. Soient K un corps et $\varphi_K : \mathbb{Z} \to K$ comme précédemment,
- si $\mathrm{Ker}\varphi_K = \{0\}$, on dit que le corps K est de caractéristique 0 (ou parfois infinie) ou d'exposant caractéristique 1,
- si $\mathrm{Ker}\varphi_K = p\mathbb{Z}$, où p est un nombre premier, on dit que K est de caractéristique p ou d'exposant caractéristique p.

Les corps de caractéristiques les nombres premiers sont dits de caractéristiques positives.

Exemple 1.2.2. Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0, si p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

Soit K un corps, de caractéristique 0, alors le morphisme $\varphi_K : \mathbb{Z} \to K$ se prolonge en une application

$$\tilde{\varphi}_K : \mathbb{Q} \to K,$$

qui à la fraction a/b associe $\varphi_K(a)/\varphi_K(b) \in K$; on voit facilement que $\tilde{\varphi}_K$ est un morphisme de corps, donc K *contient le sous-corps* $\tilde{\varphi}_K(\mathbb{Q})$ *qui est isomorphe au corps des nombres rationnels* $\mathbb{Q}$.

Soit K un corps de caractéristique $p > 0$. Alors φ_K induit un morphisme

$$\overline{\varphi}_K : \frac{\mathbb{Z}}{\mathrm{Ker}\varphi_K} = \frac{\mathbb{Z}}{p\mathbb{Z}} \to K,$$

par conséquent K *contient le corps* $\overline{\varphi}_K(\mathbb{Z}/p\mathbb{Z})$*, qui a* p *éléments, qui est isomorphe au corps* $\mathbb{Z}/p\mathbb{Z}$ (un corps à p éléments est souvent noté $\mathbb{F}_p$).

Définition 1.2.3. Soit K un corps de caractéristique 0 (resp. $p > 0$), alors le sous-corps $\tilde{\varphi}_K(\mathbb{Q})$ (resp. $\overline{\varphi}_K(\mathbb{Z}/p\mathbb{Z})$) s'appelle le sous-corps premier de K, il est isomorphe à $\mathbb{Q}$ (resp. $\mathbb{Z}/p\mathbb{Z}$).

Proposition 1.2.4. *Soit* L/K *une extension de corps, alors* K *et* L *ont même caractéristique.*

Démonstration. Comme le diagramme

$$\begin{array}{ccc} K & \subseteq & L \\ {\scriptstyle \varphi_K}\uparrow & & \nearrow_{\varphi_L} \\ & \mathbb{Z} & \end{array}$$

est commutatif, on voit que $\mathrm{Ker}\varphi_K$=$\mathrm{Ker}\varphi_L$. □

1.3 Extensions algébriques

Définition 1.3.1. Soit L/K une extension. Un élément x de L est dit algébrique sur K s'il existe un polynôme $P \in K[X]$, qui ne soit pas le polynôme nul, tel que $P(x) = 0$. Sinon on dit que x est transcendant sur K. L'extension L/K est dite algébrique (on dit aussi que L est algébrique sur K) si tout élément de L est algébrique sur K.

Soient, comme dans la définition, L/K une extension et x un élément de L. L'ensemble I_x des polynômes $P \in K[X]$ tels que $P(x) = 0$ est un idéal de l'anneau des polynômes $K[X]$, c'est un idéal principal car l'anneau $K[X]$ est principal. On a $I_x = \{0\}$ dans le cas où x est transcendant sur K. Si $I_x \neq 0$, parmi tous ses générateurs, il en existe un qui est un polynôme unitaire, c'est à dire un polynôme dont le coefficient du terme de plus haut degré (appelé aussi coefficient dominant) est égal à 1.

Définition 1.3.2. Soient L/K une extension et x un élément de L, algébrique sur K. On désigne par $\mathrm{irr}(x, K; X)$ le générateur unitaire de

$$I_x = \{P \in K[X] \ / \ P(x) = 0\}.$$

Le polynôme $\mathrm{irr}(x, K; X)$ s'appelle le polynôme minimal de x sur K.

Théorème 1.3.3. *Soit L/K une extension et soit $x \in L$.*
(i) Alors x est algébrique sur K si et seulement si l'extension $K(x)/K$ est finie (donc si et seulement si $[K(x) : K]$ est fini).
(ii) Supposons x algébrique sur K, alors $\mathrm{irr}(x, K; X)$ est un élément irréductible de $K[X]$, $[K(x) : K] = \deg \mathrm{irr}(x, K; X)$ et $K[x] = K(x)$.

Démonstration. Supposons que x soit algébrique sur K, soit $\varphi : K[X] \to L$ l'application qui à tout $P \in K[X]$ associe $P(x)$. C'est un morphisme d'anneaux unitaires et, clairement, l'image de φ est le sous-anneau $K[x]$ de L. Le noyau de φ est, par définition, l'idéal $(\mathrm{irr}(x, K; X))$ de $K[X]$. On a donc l'isomorphisme (canonique) d'anneaux

$$\frac{K[X]}{(\mathrm{irr}(x, K; X))} \simeq K[x].$$

Ceci prouve que l'idéal $(\mathrm{irr}(x, K; X))$ est premier (car l'image de φ est intègre), donc que le polynôme $\mathrm{irr}(x, K; X)$ est irréductible, par suite que $K[X]/(\mathrm{irr}(x, K; X))$ est un corps. Par conséquent $K[x]$ est un corps. Enfin, la division euclidienne montre que pour tout élément P de $K[X]$ il existe un unique $R \in K[X]$ tel que

$$\deg R < \deg \mathrm{irr}(x, K; X) \text{ et } P - R \in (\mathrm{irr}(x, K; X))$$

(on fait la convention $\deg 0 = -\infty$). Soit d le degré de $\mathrm{irr}(x, K; X)$, ce qui précède montre que l'image canonique de $\{1, X, X^2, \cdots, X^{d-1}\}$ dans le quotient $K[X]/(\mathrm{irr}(x, K; X))$ en est une base sur K.

Il reste à prouver la réciproque de (i). Supposons l'extension $K(x)/K$ finie et posons $d = [K(x) : K]$. Alors la famille $\{1, x, \cdots, x^{d-1}, x^d\}$ est liée sur K, puisqu'elle possède $d + 1$ éléments distincts, donc il existe $a_0, a_1, \cdots, a_d$ appartenant à K, non tous nuls, tels que

$$\sum_{0 \le i \le d} a_i x^i = 0,$$

par conséquent, x est algébrique sur K. □

Remarque 1.3.4. Soient L/K une extension et $x \in L$ algébrique sur K. On a mis en évidence dans cette démonstration le morphisme $\varphi : K[X] \to L$, qui à tout $P \in K[X]$ associe $P(x)$, et l'isomorphisme

$$\frac{K[X]}{(\mathrm{irr}(x, K; X))} \simeq K(x) = K[x]$$

qui s'en déduit. Ils sont intéressants en soi et nous seront utiles d'autres fois. Il résulte aussi de la démonstration que $\{1, x, x^2, \cdots, x^{d-1}\}$ est une K-base de $K(x)$.

Le théorème 1.3.3 admet plusieurs conséquences, que nous regroupons en le corollaire suivant.

Corollaire 1.3.5. *Soit L/K une extension de corps.*
(i) Soit M une partie de L formée d'éléments algébriques sur K, alors l'extension $K(M)/K$ est algébrique et l'on a $K[M] = K(M)$; si de plus M est finie, alors $K(M)/K$ est une extension finie.
(ii) Soit E l'ensemble des éléments de L algébriques sur K, alors E est un sous-corps de L (c'est une extension algébrique de K).
(iii) Soit E un corps intermédiaire entre K et L (on a donc les inclusions entre corps et sous-corps $K \subset E \subset L$), alors l'extension L/K est algébrique si et seulement si les deux extensions L/E et E/K le sont.
(iv) Supposons que L/K soit une extension finie, alors c'est une extension algébrique.

Démonstration. (i) Soit $x \in K(M)$. Par définition de $K(M)$ (voir aussi la proposition 1.1.9) il existe des éléments $y_1, \cdots, y_d$ de M, en nombre fini, tels que $x \in K(y_1, \cdots, y_d)$. Alors chaque y_i, $1 \leq i \leq d$, est algébrique sur K, donc à plus forte raison sur $K(y_1, \cdots, y_{i-1})$, $2 \leq i \leq d$. Il vient en itérant 1.1.5 que l'extension $K(y_1, \cdots, y_d)/K$ est finie, par suite que $K(x)$ est un K -espace vectoriel de dimension finie (car c'est un sous-K espace vectoriel de $K(y_1, \cdots, y_d)$), ce qui prouve que x algébrique sur K. On a $K[M] = K(M)$, en effet, soit $x \in K[M]$, $x \neq 0$, comme $K[x] = K(x)$ on a $x^{-1} \in K[M]$, donc $K[M]$ est un corps. Enfin, si M est finie, $M = \{y_1, \cdots, y_d\}$, les arguments précédents montrent que $K(M)/K$ est finie.

(ii) D'après (i), $K(E)/K$ est une extension algébrique, donc $K(E) \subset E$, dont il résulte $K(E) = E$.

(iii) Si L/K est algébrique. Alors les éléments de L sont algébriques sur E, puisqu'ils annulent des polynômes non nuls à coefficients dans K, donc dans E. Les éléments de E sont aussi des éléments de L, donc sont algébriques sur K.

Si L/E et E/K sont algébriques. Soit $x \in L$ et soit $\mathrm{irr}(x, E, X) = X^d + a_1 X^{d-1} + \cdots + a_d$, avec donc $a_1, \cdots, a_d$ dans E. Considérons les extensions

$$K \subset K(a_1, \cdots, a_d) \subset K(x, a_1, \cdots, a_d).$$

Comme les a_i sont dans E, ils sont algébriques sur K, donc $K(a_1, \cdots, a_d)/K$ est une extension finie (cf. (i) de ce corollaire). De plus , x est algébrique sur $K(a_1, \cdots, a_d)$, par définition des a_i, donc $K(x, a_1, \cdots, a_d)/K(a_1, \cdots, a_d)$ est aussi une extension finie (cf. le théorème 1.3.3). Ainsi $K(x, a_1, \cdots, a_d)/K$ est une extension finie, donc $K(x)/K$, qui en est une sous-extension, est finie et on applique encore le théorème.

(iv) Soit $x \in L$. Comme $K(x)$ est un sous-K-espace vectoriel de L, il est de dimension finie. □

1.4 Corps de ruptures

L'objet de ce paragraphe est de démontrer le théorème suivant.

Théorème 1.4.1. *Soient K un corps et $P(X)$ un élément de $K[X]$ n'appartenant pas à K. Alors il existe une extension L de K dans laquelle P admet une racine.*

Démonstration. On peut supposer $P(X)$ irréductible dans $K[X]$, quitte à le remplacer par l'un de ses diviseurs. Soit

$$s : K[X] \to E = \frac{K[X]}{(P(X))}$$

la surjection canonique de $K[X]$ sur son quotient E par l'idéal $(P(X))$. Soit σ la restriction de s à K, soit $P^\sigma(T) \in E[T]$ le polynôme obtenu à partir de P par l'action de σ sur ses coefficients [1]. Le polynôme P^σ a une racine dans E car

$$P^\sigma(s(X)) = s(P(X)) = 0,$$

mais $\sigma : K \hookrightarrow E$ n'est pas une inclusion, E n'est pas une extension de K.

Construisons une extension L de K qui soit isomorphe à E et dans laquelle P a une racine. Selon le lemme suivant, il existe un ensemble F qui est disjoint de K et en bijection avec $E - \sigma(K)$, le complémentaire de $\sigma(K)$ dans E. Soit $\varphi : F \to (E - \sigma(K))$ cette dernière bijection et soit $L = K \cup F$. L'ensemble L est en bijection avec E par l'application ψ ainsi définie : soit $x \in L$, on pose $\psi(x) = \sigma(x)$ si $x \in K$ et $\psi(x) = \varphi(x)$ si $x \in F$. On fait de L un corps, extension de K, par transport de structure, c'est à dire par les lois : pour tous $x, y \in L$

$$x + y = \psi^{-1}(\psi(x) + \psi(y)),$$

$$x \cdot y = \psi^{-1}(\psi(x) \cdot \psi(y)).$$

Alors $\psi^{-1}(s(X))$ est une racine de P dans L. □

Lemme 1.4.2. *Soient A et B deux ensembles, alors il existe un ensemble C disjoint de A et en bijection avec B.*

Démonstration. La démonstration donnée ici nous a été communiquée par notre collègue Anne BAUVAL. Désignons par Z la réunion des ensembles qui sont des éléments de A et soit X l'ensemble des éléments u de Z qui n'admettent pas eux-même comme élément :

$$X = \{u \in Z \ / \ u \notin u\}.$$

[1] On a $\sigma : K \to E$, si $P(X) = \sum_{1 \leq i \leq d} a_i X^i \in K[X]$ alors $P^\sigma(X) = \sum_{1 \leq i \leq d} \sigma(a_i) X^i \in E[X]$. Nous utiliserons plusieurs fois cette notation.

Montrons $X \notin Z$. En effet, on a pour tout $u \in Z$

$$u \in X \iff u \notin u,$$

donc si $X \in Z$, on aurait

$$X \in X \iff X \notin X$$

ce qui est faux.

Soit $C = \{\{X, b\} \ / \ b \in B\}$. Il est clair que C est en bijection avec B. Il reste à prouver que $C \cap A = \emptyset$: s'il existe $b \in B$ tel que $\{X, b\} \in A$, alors, par définition de Z, on a $\{X, b\} \subset Z$, donc $X \in Z$, ce qui est faux. □

Définition 1.4.3. Soient K un corps et $P(X)$ un élément de $K[X]$ n'appartenant pas à K. Une extension algébrique L de K dans laquelle $P(X)$ possède une racine s'appelle un corps de rupture sur K de $P(X)$.

Remarque 1.4.4. Soient K un corps et $P(X)$ un élément de $K[X]$ n'appartenant pas à K. Le théorème 1.4.1 prouve donc que $P(X)$ possède toujours un corps de rupture L sur K, la démonstration ainsi que 1.3.4 montrent, lorsque $P(X)$ est irréductible sur K, que l'on peut choisir ce corps de rupture L et une racine x de $P(X)$ dans L tels que

$$L = K(x) \simeq \frac{K[X]}{(P(X))},$$

l'isomorphisme associant x à la classe de X.

1.5 Clôtures algébriques

Proposition 1.5.1. *Soit K un corps, les assertions suivantes sont équivalentes.*
(i) Tout élément de $K[X]$ qui n'est pas dans K admet une racine dans K.
(ii) Tout élément de $K[X]$ qui n'est pas dans K se décompose en un produit de polynômes du premier degré, autrement dit, les éléments irréductibles de $K[X]$ sont les polynômes du premier degré.
(iii) Le corps K n'admet pas d'extension algébrique non triviale (c'est à dire distincte de lui-même).

Démonstration. (i) implique (ii). Soit $P(X) \in K[X]$ un polynôme non constant. Il possède une racine α dans K, donc il s'écrit $P(X) = (X - \alpha)Q(X)$ avec $Q(X) \in K[X]$. On a $\deg Q = \deg P - 1$. Par récurrence sur le degré de $P(X)$ on prouve donc (ii).

(ii) implique (iii). Soient L/K une extension algébrique, $x \in L$ et $P(X) = \mathrm{irr}(x, K; X)$. D'après (ii), $P(X)$ s'écrit dans $K[X]$ sous la forme $K[X] = \prod_{1 \leq i \leq d}(X - x_i)$, avec $x_i \in K$ et $d = \deg P$. Les racines de $P(X)$ dans L sont

encore les x_i, $1 \leq i \leq d$, x est l'une de ces racines et est donc dans K. Ceci implique $d = 1$.

(iii) implique (i). Soit $P(X) \in K[X]$ un polynôme non constant. Soit L un corps de rupture de $P(X)$ sur K (cf. 1.4.1 et 1.4.3). On a d'après (iii) $L = K$, donc $P(X)$ possède une racine dans K. □

Cette proposition conduit à la définition

Définition 1.5.2. Un corps K vérifiant l'une des assertions de la proposition 1.5.1 est dit algébriquement clos.

Exemple 1.5.3. Le corps des nombres complexes $\mathbb{C}$ est algébriquement clos. les corps des rationnels $\mathbb{Q}$ et des réels $\mathbb{R}$ ne sont pas algébriquement clos, de même les corps finis (si $\mathbb{F}$ est un corps fini, alors le polynôme $1+\prod_{\lambda\in\mathbb{F}}(X-\lambda)$ n'a pas de racine dans $\mathbb{F}$).

La suite de ce paragraphe consiste à prouver que pour tout corps K, "il existe un plus petit corps Ω algébriquement clos, le contenant et unique pour ces propriétés". Cette formulation est imprécise, mais l'idée s'énonce rigoureusement comme suit.

Définition 1.5.4. Soit K un corps, on appelle clôture algébrique de K tout corps Ω qui est une extension algébrique de K et qui est aussi algébriquement clos.

Théorème 1.5.5. *Soit K un corps.*
(i) Le corps K possède une clôture algébrique.
(ii) Soit Ω une clôture algébrique de K, alors pour tout morphisme $\sigma : K \to L$, où L est un corps algébriquement clos, il existe un morphisme $\tau : \Omega \to L$ qui prolonge σ.
(iii) Deux clôtures algébriques de K sont K-isomorphes.

La démonstration se fait en plusieurs étapes.

Lemme 1.5.6. *Soit K un corps, alors il existe une extension L de K dans laquelle tout élément P de $K[X]$, $P \notin K$, possède une racine.*

Démonstration. Elle est due à Emil ARTIN. Soit

$$\mathfrak{K} = K[X_P \ / \ P \in K[X] - K],$$

c'est à dire que $\mathfrak{K}$ est l'anneau des polynômes à coefficients dans K et en les indéterminées $\{X_P\}$ indexées sur l'ensemble des P de $K[X]$ non constants, on peut le voir comme une réunion d'anneaux de polynômes à un nombre fini de variables :

$$\mathfrak{K} = \bigcup_{F\subset\{X_P\}_{P\in K[X]-K}, F\,fini} K[X_P \ / \ P \in F].$$

Soit $\mathfrak{I}$ l'idéal de $\mathfrak{K}$ engendré par $\{P(X_P)\ /P \in K[X] - K\}$.

Montrons $\mathfrak{I} \neq \mathfrak{K}$. Sinon, il existe une relation du type

$$Q_1 P_1(X_{P_1}) + \cdots + Q_r P_r(X_{P_r}) = 1$$

avec les Q_i dans $\mathfrak{K}$. Cette relation ne fait intervenir qu'un nombre fini d'indéterminées que l'on note $T_1, \cdots, T_n$, avec $T_i = X_{P_i}$ pour $1 \leq i \leq r$, elle s'écrit donc dans $K[T_1, \cdots, T_n]$

$$(*) \qquad \sum_{1 \leq i \leq r} Q_i(T_1, \cdots, T_n) P_i(T_i) = 1.$$

Soit E une extension de K dans laquelle chaque P_i a une racine, notée α_i, $1 \leq i \leq r$ (cf. 1.4.1, c'est à dire que l'on considère une extension E_1 de K dans laquelle P_1 a une racine, puis une extension E_2 de E_1 dans laquelle P_2 a une racine... ; avec ces notations on prend $E = E_r$). Soit $\varphi : K[T_1, \cdots, T_n] \to E$ le morphisme de K-algèbres qui à T_i associe α_i. En appliquant φ à $(*)$ il vient $1 = 0$ dans E, ce qui est faux. Par conséquent $\mathfrak{I} \neq \mathfrak{K}$.

Comme $\mathfrak{I} \neq \mathfrak{K}$, il existe un idéal maximal $\mathfrak{M}$ de $\mathfrak{K}$ contenant $\mathfrak{I}$. Soient $E = \mathfrak{K}/\mathfrak{M}$ et $s : \mathfrak{K} \to E$ la surjection canonique, notons σ la restriction de s à K. Soit P un polynôme non constant à coefficient dans K. On a $0 = s(P(X_P) = P^\sigma(s(X_P))$ (la notation P^σ est expliquée dans la note de bas de page suivant la démonstration de 1.4.1), donc P^σ a une racine dans le corps E, quel que soit P. Il suffit alors de répéter la fin de la démonstration de 1.4.1 pour obtenir un corps L (isomorphe à E), extension de K et dans lequel tout élément non constant de $K[X]$ a une racine. □

Lemme 1.5.7. *Soit K un corps, alors il existe un corps L qui est une extension algébrique de K et un corps algébriquement clos.*

Démonstration. Soit L_1 une extension de K dans laquelle tout élément non constant de $K[X]$ a une racine (cf. le lemme précédent), de même soit L_2 une extension de L_1 dans la quelle les polynômes non constants de $L_1[X]$ ont une racine... On construit ainsi, par récurrence, une suite $(L_n)_{n \in \mathbb{N}}$ de corps tels que $L_0 = K$ et que L_{n+1} soit une extension de L_n dans laquelle tous les éléments non constants de $L_n[X]$ ont une racine. Soit $L_\infty = \cup_{n \in \mathbb{N}} L_n$, c'est une extension de K. Désignons par L l'ensemble des éléments de L_∞ algébriques sur K, c'est une extension algébrique de K (cf. (ii) de 1.3.5). Montrons que L est algébriquement clos. Soit $P(X) = a_0 + a_1 X + \cdots + a_d x^d \in L[X]$ un polynôme non constant (avec donc les a_i dans L). Les a_i sont dans L_∞, donc il existe $n \in \mathbb{N}$ tel que $P(X) \in L_n[X]$, par suite $P(X)$ a une racine dans L_{n+1}, donc dans L_∞, que l'on appelle α. Les deux extensions

$$K \subset K(a_0, a_1, \cdots, a_d) \subset K(\alpha, a_0, a_1, \cdots, a_d)$$

sont algébriques, la première car les a_i sont dans L, la seconde parce que α est racine de $P(X) \in K(a_0, a_1, \cdots, a_d)[X]$, donc α est algébrique sur K (cf.

(iii) de 1.3.5). Par conséquent α est dans L_∞ et est algébrique sur K, il est donc dans L. Ceci prouve que L est algébriquement clos (cf. (i) de 1.5.1). □

Nous avons donc montré la partie (i) du théorème 1.5.5, la fin de la démonstration nécessite le résultat important suivant.

Proposition 1.5.8. *Soient E/K une extension algébrique et $\sigma : K \to L$ un morphisme dans le corps algébriquement clos L. Alors il existe un prolongement $\tau : E \to L$ de σ à E.*

Démonstration. Soit $\mathcal{S}$ l'ensemble des couples (F, τ) tels que F soit un corps intermédiaire entre K et E et que τ prolonge σ à F.
- L'ensemble $\mathcal{S}$ est non vide car $(K, \sigma) \in \mathcal{S}$.
- Pour des éléments de $\mathcal{S}$, on écrit $(F, \tau) < (F', \tau')$ si $F \subset F'$ et si τ' prolonge τ à F'. Ceci est un ordre sur $\mathcal{S}$.

Pour cet ordre $\mathcal{S}$ est inductif. En effet, soit $((F_n, \tau_n))_{n\in\mathbb{N}}$ une suite croissante d'éléments de $\mathcal{S}$, alors sa borne supérieure est l'élément $(F_\infty = \cup_{n\in\mathbb{N}} F_n, \tau_\infty)$ de $\mathcal{S}$, où τ_∞ est défini par la relation : pour tout $n \in \mathbb{N}$ la restriction de τ_∞ à F_n est τ_n.

Donc $\mathcal{S}$ est inductif et non vide, par suite, d'après le lemme de ZORN, il possède un élément maximal, que l'on note (F, τ). Il reste à prouver que $F = E$, c'est une conséquence de la maximalité de (F, τ) et du lemme suivant appliqué à l'extension $F(x)/F$, pour un éventuel élément x de $E - F$. □

Lemme 1.5.9. *Soit $\tau : F \to L$ un morphisme d'un corps F dans un corps algébriquement clos L. Soit E/F une extension et $x \in E$ algébrique sur F. Alors τ admet un prolongement à $F(x)$.*

Démonstration. Soit $P(X) = \mathrm{irr}(x, F; X)$ et soit y une racine dans L du polynôme $P^\tau(X)$. Soit

$$\varphi : F[X] \to L$$

le morphisme qui à $Q(X) \in F[X]$ associe $Q^\tau(y)$, son noyau est l'idéal $(P(X))$. Soit

$$\overline{\varphi} : \frac{F[X]}{(P(X))} \to L$$

le morphisme qui s'en déduit, soit aussi

$$\theta : F(x) \simeq \frac{F[X]}{(P(X))}$$

l'isomorphisme de 1.3.4, alors $\overline{\varphi} \circ \theta$ répond à la question. □

Il ne reste plus qu'à montrer l'assertion (iii) du théorème 1.5.5. Soient Ω_1 et Ω_2 deux clôtures algébriques de K. D'après (ii) de 1.5.5 l'inclusion $K \subset \Omega_2$ se prolonge en un K-homomorphisme $\sigma_1 : \Omega_1 \to \Omega_2$, de même $K \subset \Omega_1$ se prolonge en un K-homomorphisme $\sigma_2 : \Omega_2 \to \Omega_1$. le lemme suivant montre que $\sigma_2^{-1} \circ \sigma_1$ est un automorphisme de Ω_1, ce qui permet de conclure.

Lemme 1.5.10. *Soit L/K une extension algébrique et soit σ un K-endomorphisme de L. Alors σ est un automorphisme.*

Démonstration. Il faut montrer que σ est surjectif. Soit $x \in L$ et soit $P(X) = \mathrm{irr}(x, K; X)$. Soit R l'ensemble des racines de P dans L et soit $y \in R$. On a $P(y) = 0$, par suite $P(\sigma(y)) = \sigma(P(y)) = 0$ (la première égalité vient du fait que les coefficients de P sont dans K, donc $P^\sigma = P$). Donc $\sigma(y)$ est une racine de P. Par suite, la restriction de σ à R est une application de R dans lui-même, qui est injective, donc surjective puisque R est fini. Ainsi x est dans l'image de σ. □

La proposition suivante est utile, bien qu'elle ne soit guère plus qu'une remarque.

Proposition 1.5.11. *Soit L/K une extension, où le corps L est algébriquement clos. Alors L contient une unique clôture algébrique de K, qui est l'ensemble Ω des éléments de L algébriques sur K.*

Démonstration. La définition de Ω implique l'unicité. Avec l'assertion (ii) de 1.3.5 on voit qu'il reste à prouver que Ω est algébriquement clos. Soit $P(X) = a_0 + a_1 X + \cdots + a_d X^d \in \Omega[X]$ un polynôme non constant. Soit α une racine de $P(X)$ dans L. Les deux extensions

$$K \subset K(a_0, a_1, \cdots, a_d) \subset K(\alpha, a_0, a_1, \cdots, a_d)$$

sont algébriques, la première car les a_i sont dans Ω, la seconde parce-que α est racine de $P(X) \in K(a_0, a_1, \cdots, a_d)[X]$, donc α est algébrique sur K (cf. (iii) de 1.3.5), c'est à dire $\alpha \in \Omega$. Ceci prouve que Ω est algébriquement clos (cf. (i) de 1.5.1). □

Exemple 1.5.12. Le corps $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ (nous le démontrerons), c'est un des rares cas aussi explicites. Par exemple, on ne sait pas décrire les clôtures algébriques de $\mathbb{Q}$, même celle contenue dans $\mathbb{C}$.

Remarque 1.5.13. Soient E/K une extension, x un élément de E algébrique sur K et $\sigma : K \to L$ un morphisme dans un corps algébriquement clos. Soit $P(X) = \mathrm{irr}(x, K; X)$. Alors, le nombre de prolongements de σ à $K(x)$ est égal au nombre de racines *distinctes* de P^σ dans L. Plus précisément, un prolongement τ de σ à $K(x)$ est complètement caractérisé par la donnée de $\tau(x)$, qui décrit l'ensemble des racines *distinctes* de P^σ dans L. Ceci se voit dans la démonstration de 1.5.9, où le choix de y est arbitraire parmi les racines de P^σ dans L. Nous reviendrons plus tard sur ce très important phénomène. Une dernière chose, sur laquelle nous reviendrons aussi, est de remarquer que le nombre de racines distinctes de P^σ dans L peut être strictement plus petit que son degré, bien que P^σ soit irréductible dans $K[X]$. Par exemple, soit p un nombre premier et soit $K = \mathbb{F}_p(T)$ un corps de fractions rationnelles à coefficients dans le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, alors le polynôme

$P(X) = X^p - T \in K[X]$ est irréductible dans $K[X]$ et, dans une clôture algébrique K^{alg} de K, il n'a qu'une seule racine (si $\alpha \in K^{\text{alg}}$ est une racine de P, on a $P(X) = X^p - \alpha^p = (X - \alpha)^p$ dans $K^{\text{alg}}[X]$). Ce phénomène ne se produit pas en caractéristique zéro.

1.6 Exercices

Exercice 1.1. 1) Montrer que les idéaux d'un corps K sont triviaux, i.e. égaux à $\{0\}$ ou à K.

2) Montrer qu'un morphisme de corps $\varphi : K \to L$ est ou bien nul, ou bien injectif ; dans le deuxième cas, montrer que $\varphi(1_K) = 1_L$.

Exercice 1.2. Soit A un anneau. S'il existe un entier $n \in \mathbb{N} \setminus \{0\}$ tel que $\forall a \in A$, $na = 0$, on appelle **la caractéristique de** A le plus petit entier $p > 0$ tel que $\forall a \in A$, $pa = 0$. S'il n'existe pas de tel n, on dit que **la caractéristique de** A est 0. On note $\mathrm{car}(A)$ la caractéristique de A.

Soit A un anneau unitaire.

1) Montrer que $\varphi : \mathbb{Z} \to A$, $n \mapsto n1_A$ est un morphisme d'anneaux.

2) Soit $\ker(\varphi) = p\mathbb{Z}$ (car c'est un idéal de l'anneau $\mathbb{Z}$ d'après 1)), montrer que $\mathrm{car}(A) = p$. En particulier, si $p > 0$, p est le plus petit entier > 0 tel que $p1_A = 0$.

3) Si A n'a pas de diviseurs de zéro (par exemple si A est intègre) et si $\mathrm{car}(A) = p > 0$, alors p est un nombre premier.

4) Quelle est la caractéristique de (i) $\mathbb{Z}$, (ii) $\mathbb{Z}/n\mathbb{Z}$, (iii) $\mathbb{C}$?

Exercice 1.3. Soit K un corps à q éléments et de caractéristique p. Montrer que p est un nombre premier et que q est une puissance de p.

Exercice 1.4. Soient A un anneau commutatif de caractéristique un nombre premier $p > 0$ et $a, b \in A$.

1) Montrer que $(a + b)^p = a^p + b^p$.

2) Montrer que l'application $F : A \to A$, $a \mapsto a^p$ est un morphisme d'anneaux (appelé **le morphisme de Frobenius**).

Exercice 1.5. Les nombres complexes suivants sont-ils conjugués sur $\mathbb{R}$? sur $\mathbb{Q}$? (a) i et $\sqrt{2}$; (b) $i + \sqrt{2}$ et $i - \sqrt{2}$.

Exercice 1.6. Soient $x = \sqrt{2}$ et $y = 1 - \sqrt{2}$. Montrer que $\mathbb{Q}(x) = \mathbb{Q}(y)$ et que $\mathrm{irr}(x, \mathbb{Q}) \neq \mathrm{irr}(y, \mathbb{Q})$.

Exercice 1.7. Soient F un corps fini à q éléments, K une extension de F et $f : F \to K$ une application. Montrer que

$$\forall x \in F,\ f(x) = \sum_{a \in F} (f(a)(1 - (x - a)^{q-1})),$$

c'est-à-dire f est polynômiale.

Exercice 1.8. 1) Soit A un anneau intègre unitaire admettant comme sous-anneau un corps K tel que A soit un K-espace vectoriel de dimension finie. Montrer que A est un corps.

2) Soient L/K une extension algébrique de corps et A un sous-anneau de L contenant K. Montrer que A est un corps. La réciproque ?

Exercice 1.9. Montrer que (i) $[L : K] = 1 \iff L = K$; (ii) Si $[L : K]$ est un nombre premier, alors l'extension L/K n'a pas de sous-extension non triviale.

Exercice 1.10. Soient α une racine dans $\mathbb{C}$ de l'équation $x^3 + x^2 + x + 2 = 0$ et $E = \mathbb{Q}(\alpha)$. Exprimer $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ et $(\alpha^2 - 1)^{-1}$ sous la forme $a\alpha^2 + b\alpha + c$ avec $a, b, c \in \mathbb{Q}$.

Exercice 1.11. Trouver tous les sous-corps intermédiaires de l'extension $\mathbb{Q}(\sqrt[4]{7})$ de $\mathbb{Q}$. (**Remarque.** On pourra refaire cet exercice avec le théorème fondamental de la théorie de Galois. voir exercice 4.2)

Exercice 1.12. Soit $X^n - a \in K[X]$ irréductible et u une racine dans une extension de K. Soit $m|n$. Montrer que $[K(u^m) : K] = \frac{n}{m}$. Quel est le polynôme irréductible de u^m sur K ?

Exercice 1.13. 1) Montrer que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. En déduire $\mathrm{irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q})$.

2) Déterminer $\mathrm{irr}(\sqrt{2}+\sqrt{3}, \mathbb{Q})$. En déduire que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

3) Déterminer l'ensemble des sous-corps intermédiaires de $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

4) Déterminer le polynôme irréductible de $\sqrt{2} + \sqrt{3} + \sqrt{5}$ sur $\mathbb{Q}$.

Remarque. On pourra aussi utiliser la notion de degré de séparabilité ou le théorème fondamental de la théorie de Galois ; refaire cette exercice quand vous disposerez de ces notions.

Exercice 1.14. Soient $p > 2$ un nombre premier et $\xi = e^{\frac{2i\pi}{p}}$.

1) Vérifier que ξ est une racine de $P(X) = X^{p-1} + X^{p-2} + \cdots + 1$ et montrer que $P(X)$ est irréductible sur $\mathbb{Q}$. En déduire $[\mathbb{Q}(\xi) : \mathbb{Q}]$.

2) On pose $\alpha = \cos\frac{2\pi}{p}$.

a) Vérifier que $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\xi)$ et $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\xi)$.

b) Montrer que ξ est une racine de $X^2 - 2\alpha X + 1$. Déterminer $[\mathbb{Q}(\xi) : \mathbb{Q}(\alpha)]$ et $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

3) On pose $p = 5$.

a) Calculer $\mathrm{irr}(\alpha, \mathbb{Q})$. En déduire que $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$.

b) Calculer $\mathrm{irr}(\xi, \mathbb{Q}(i))$ et $\mathrm{irr}(\xi, \mathbb{Q}(\sqrt{5}))$.

Exercice 1.15. Soient K une extension d'un corps F et $a \in K$ tel que $[F(a) : F]$ soit impair. Montrer que $F(a) = F(a^2)$. Donner un contre exemple avec $[F(a) : F]$ pair.

Exercice 1.16. Soient α et β deux éléments d'une extension algébrique L d'un corps K. Montrer que si les degrés de $\mathrm{irr}(\alpha, K)$ et de $\mathrm{irr}(\beta, K)$ sont premiers entre eux, $\mathrm{irr}(\alpha, K) = \mathrm{irr}(\alpha, K(\beta))$. En déduire $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$.

Exercice 1.17. Soient L/K une extension de corps, E/K et F/K deux extensions intermédiaires de degré fini.

1) Montrer que $E(F)/E$ est finie et que $[E(F) : E] \leq [F : K]$. En déduire que $[E(F) : K] \leq [E : K][F : K]$. Montrer qu'on a égalité si $[E : K]$ et $[F : K]$ sont premiers entre eux.

2) Montrer que si $[E(F) : K] = [E : K][F : K]$, alors $E \cap F = K$.

3) Soient x et y deux racines distinctes de $X^3 - 2$ dans $\mathbb{C}$. Montrer que $[\mathbb{Q}(x, y) : \mathbb{Q}] < [\mathbb{Q}(x) : \mathbb{Q}][\mathbb{Q}(y) : \mathbb{Q}]$ et que $\mathbb{Q}(x) \cap \mathbb{Q}(y) = \mathbb{Q}$.

Exercice 1.18. Soient K un corps, $E = K(X)$, $R = \frac{X^3}{X+1} \in E$ et $F = K(R)$.

1) Montrer que $E = F(X)$ et que $X \notin F$.

2) Montrer que $T^3 - RT - R$ est irréductible dans $F[T]$, en déduire $[E : F]$.

Exercice 1.19. Montrer que $\mathbb{Q}$ et les corps finis ne sont pas algébriquement clos.

Exercice 1.20. (**Théorème de Liouville**) On appelle **nombre algébrique** tout nombre complexe qui est une racine d'un polynôme à coefficients dans $\mathbb{Q}$. Soit α un nombre algébrique réel de degré $n > 1$ sur $\mathbb{Q}$. Montrer qu'il existe $c = c(\alpha) > 0$ tel que $| \alpha - \frac{p}{q} | > \frac{c}{q^n}$ pour tout $\frac{p}{q} \in \mathbb{Q}$.
(Indication : Soit $P(\alpha) = 0$ avec $\deg(P) = n$ et $P(X) \in \mathbb{Z}[X]$. Utiliser $P(\alpha) - P(\frac{p}{q}) = (\alpha - \frac{p}{q})P'(\xi)$.)
Application : On appelle **nombres de Liouville** les nombres de la forme $\alpha = \sum_{k=1}^{\infty} \frac{\alpha_k}{10^{k!}}$ où $\{\alpha_k\}_{k \in \mathbb{N}}$ est une suite de chiffres ne tendant pas vers zéro.
Montrer que les nombres de Liouville sont transcendants.

Exercice 1.21. Trouver un exemple d'une extension algébrique L/K avec $[L : K] = 3$ et pour tout $a \in K$, $L \neq K(\sqrt[3]{a})$ où $\sqrt[3]{a}$ est une racine de $X^3 - a$ dans une clôture algébrique de L/K.

Chapitre 2

Corps de décomposition, extensions normales

2.1 Corps de décompositions

Définition 2.1.1. Soient K un corps et $(P_i)_{i\in I}$ une famille d'éléments de $K[X]$. Soit L une extension de K telle que
- pour tout $i \in I$, P_i se décompose dans $L[X]$ en un produit de polynômes du premier degré, c'est à dire

$$P_i(X) = \lambda_i \prod_{1\leq j\leq d_i} (X - a_{i,j})$$

avec $a_{i,j} \in L$ et $\lambda_i \in K$ (ce dernier est le coefficient dominant de P_i),
- le corps L est engendré sur K par les racines des P_i, c'est à dire

$$L = K(\{a_{i,j}\}_{i\in I, 1\leq j\leq d_i}).$$

Alors L s'appelle un corps de décomposition de la famille $(P_i)_{i\in I}$ sur K (lorsqu'il n'y a qu'un seul polynôme P, L est appelé corps de décomposition de P sur K).

Remarque 2.1.2. Soient K un corps et $(P_i)_{i\in I}$ une famille d'éléments de $K[X]$. Dans dans toute extension Ω/K, où Ω est algébriquement clos (en particulier dans toute clôture algébrique de K) il existe un corps de décomposition sur K de la famille $(P_i)_{i\in I}$, c'est le corps engendré sur K par les racines dans Ω des (P_i), $i \in I$. La définition montre ce corps est nécessairement ainsi, par suite qu'il est unique (dans tout corps algébriquement clos Ω, extension de K).

Exercice 2.1. Soit K un corps. Montrer qu'une extension L de K est une clôture algébrique de K si et seulement si c'est un corps de décomposition sur K de la famille de tous les éléments non constants de $K[X]$.

La proposition suivante énonce une propriété très forte des corps de décomposition, qui permet de préciser l'unicité énoncée à la remarque 2.1.2.

Proposition 2.1.3. *Soient K un corps et $(P_i)_{i\in I}$ une famille d'éléments de $K[X]$.*
(i) Soient L_1 et L_2 deux corps de décomposition de $(P_i)_{i\in I}$ sur K, Ω une extension de L_2 qui est un corps algébriquement clos et $\sigma : L_1 \to \Omega$ un K-homomorphisme. Alors on a $\sigma(L_1) = L_2$, c'est à dire que σ induit un K-isomorphisme entre L_1 et L_2.
(ii) Deux corps de décomposition de $(P_i)_{i\in I}$ sur K sont K-isomorphes.

Démonstration. Posons pour $i \in I$

$$P_i(X) = \lambda_i \prod_{1\leq j\leq d_i} (X - a_{i,j})$$

avec $a_{i,j} \in L_1$ et $\lambda_i \in K$. On a dans $\Omega[X]$

$$P_i^\sigma(X) = P_i(X) = \lambda_i \prod_{1\leq j\leq d_i} (X - \sigma(a_{i,j}))$$

et rappelons que L_1 est engendré sur K par les $a_{i,j}$ (cf. 2.1.1). Ainsi

$$\sigma(L_1) = K(\{\sigma(a_{i,j})\}_{i\in I, 1\leq j\leq d_i},$$

c'est à dire que $\sigma(L_1)$ est engendré sur K par les racines des P_i dans Ω, comme L_2. Ceci prouve (i). L'assertion (ii) en est une conséquence : si L_1 et L_2 sont deux corps de décomposition de $(P_i)_{i\in I}$ sur K, on prend pour Ω une clôture algébrique de L_2 et pour σ un prolongement à L_1 de l'inclusion $K \subset \Omega$ (cf. 1.5.8). □

Le théorème suivant donne des caractérisations des corps de décomposition.

Théorème 2.1.4. *Soit L/K une extension algébrique. Les assertions suivantes sont équivalentes.*
- (i) L est un corps de décomposition d'une famille d'éléments de $K[X]$.
- (ii) Pour tout corps Ω algébriquement clos, extension de L, tout K-homomorphisme de L dans Ω induit un K-automorphisme de L.
- (iii) Il existe un corps Ω algébriquement clos, extension de L, tel que tout K-homomorphisme de L dans Ω induise un K-automorphisme de L.
- (vi) Tout polynôme de $K[X]$, irréductible, qui possède une racine dans L, se décompose dans $L[X]$ en un produit de polynômes du premier degré.

Démonstration. (i) implique (ii). C'est une conséquence directe de l'assertion (i) de 2.1.3.

(ii) implique (vi). Soient Ω une clôture algébrique de K contenant L, P un élément irréductible de $K[X]$ et x une racine de P dans L. Soit y une racine de P dans Ω. Des morphismes

$$\frac{K[X]}{(P(X))} \simeq K(x) \text{ et } \frac{K[X]}{(P(X))} \simeq K(y)$$

venant de 1.3.4, on déduit un K-homomorphisme

$$\sigma : K(x) \simeq K(y) \hookrightarrow \Omega,$$

la seconde application étant une inclusion, et l'on a $\sigma(x) = y$. Soit σ' un prolongement de σ à L. On a d'après (ii) $\sigma(L) = L$, donc $y \in L$. On a montré que toutes les racines de P dans Ω sont en fait dans L. Ceci est (iii).

(vi) implique (i). Pour tout $x \in L$, soit $P_x = \mathrm{irr}(x, K; X)$. Comme chaque P_x a une racine dans L, d'après (iii) il se décompose dans $L[X]$ en un produit de polynômes du premier degré, c'est à dire que si l'on considère une clôture algébrique Ω de K contenant L, toutes les racines des P_x dans Ω sont en fait dans L. De plus il est clair que L est engendré sur K par les racines des P_x, $x \in L$, parce que l'ensemble de ces racines contient tous les éléments de L. Donc L est un corps de décomposition de la famille $(P_x)_{x\in L}$ d'éléments de $K[X]$.

(iii) implique (ii). Soit Ω donné par (ii). Soient Ω' un corps algébriquement clos, extension de L et $\sigma : L \to \Omega'$ un K-homomorphisme. Soient Ω_a et Ω'_a l'ensemble des éléments de Ω et Ω' respectivement algébriques sur L, ce sont des clôtures algébriques de L et de K (cf. 1.5.11). Soit $\tau : \Omega_a \to \Omega'_a$ un prolongement de σ, c'est un isomorphisme (cf. 1.5.5). On a $\tau^{-1} \mid L$ qui est un K-homomorphisme de L dans Ω, donc $\tau^{-1}(L) = L$, par suite $\tau(L) = L$, ce qui s'écrit $\sigma(L) = L$. □

2.2 Extensions normales

Définition 2.2.1. Une extension algébrique L/K satisfaisant l'une des conditions équivalentes du théorème 2.1.4 est dite normale (ou quasi-galoisienne) On dit aussi que L est normal (ou quasi-galoisien) sur K.

La proposition suivante donne quelques propriétés de ces extensions.

Proposition 2.2.2. *Soit K un corps.*
(i) Soient L/K et E/L deux extensions (donc $K \subset L \subset E$), alors si le corps E est normal sur K, il est normal sur L.
(ii) Soit E une extension de K. Soit $(L_i)_{i\in I}$ une famille de sous-corps de E, chacun étant une extension normale de K, alors $\bigcap_{i\in I} L_i$ est une extension normale de K.
(iii) Soient L_1 et L_2 deux corps, extensions normales de K, qui sont des sous-corps d'un même troisième corps E, alors le compositum $L_1 \cdot L_2$ est une extension normale de K.

Démonstration. (i) Soit Ω un corps algébriquement clos, extension de E et soit $\sigma : E \to \Omega$ un L-homomorphisme, il faut prouver que $\sigma(E) = E$ (cf. (ii) de 2.1.4), mais ceci est vrai à cause de l'hypothèse, puisque σ est à plus forte raison un K-homomorphisme.

(ii) Posons $F = \bigcap_{i\in I} L_i$. Soit E^{alg} une clôture algébrique de E. Soit P un élément irréductible de $K[X]$ ayant une racine x dans F. Dans $E^{\text{alg}}[X]$ on peut écrire

$$P(X) = \lambda \prod_{1\leq j\leq d} (X - x_i)$$

avec par exemple $x = x_1$. Comme L_i contient x, il contient tous les x_j, $1 \leq j \leq d$ (car L_i/K est normale, cf. (iii) de 2.1.4). Ceci est vrai pour tout $i \in I$, donc F contient tous les x_i, $1 \leq i \leq d$.

(iii) Soit Ω un corps algébriquement clos, extension de $L_1 \cdot L_2$ et soit $\sigma : L_1 \cdot L_2 \to \Omega$ un K-homomorphisme. Comme L_1/K est normale on a $\sigma(L_1) = L_1$ (cf. (ii) de 2.1.4), de même pour L_2. Il vient $\sigma(L_1 \cdot L_2) = L_1 \cdot L_2$. □

Remarque 2.2.3. La réciproque de l'assertion (i) de 2.2.2 est *fausse*, c'est à dire que si l'on a deux extensions

$$K \subset L \subset E$$

avec L/K et E/L normales, alors il peut se faire que E/K ne soit pas normale. Par exemple $\mathbb{Q}(\sqrt{2})$ est une extension normale de $\mathbb{Q}$, car c'est un corps de décomposition sur $\mathbb{Q}$ de $X^2 - 2$, $\mathbb{Q}(\sqrt[4]{2})$ est une extension normale de $\mathbb{Q}(\sqrt{2})$ car c'est un corps de décomposition sur $\mathbb{Q}(\sqrt{2})$ de $X^2 - \sqrt{2}$, mais $\mathbb{Q}(\sqrt[4]{2})$ n'est pas une extension normale de $\mathbb{Q}$.

L'assertion (ii) de 2.1.4 dit qu'étant donnée une extension normale L/K, tout K- homomorphisme de L dans un corps algébriquement clos le contenant, est en fait un K-automorphisme de L. Cette propriété est au coeur de la théorie de Galois.

Définition 2.2.4. Soit L/K une extension normale. Le groupe $\text{End}_K(L)$ (pour la composition des applications) des K-automorphismes de L s'appelle le groupe de Galois de L sur K, on le note $\text{Gal}(L/K)$.

2.3 Fermetures normales

Proposition 2.3.1. *Soit L/K une extension algébrique.*
(i) Soit Ω une extension algébriquement close de K contenant L. Alors il existe un plus petit sous-corps N de Ω contenant L et normal sur K.
(ii) Soient Ω et Ω' deux extensions algébriquement closes de K contenant L, soient N et N' les corps mis en évidence en (i), pour Ω et Ω' respectivement. Alors N et N' sont L-isomorphes.

Démonstration. Soit $N = \bigcap E$, où E décrit l'ensemble des sous-corps de Ω tels que $L \subset E$ et E normal sur K. L'ensemble de ces sous-corps est non vide car l'un d'entre eux est la clôture algébrique de K contenue dans Ω (cf. 1.5.11). D'après l'assertion (ii) de 2.2.2, l'extension N/K est normale, de plus il est clair que c'est la plus petite contenant L et incluse dans Ω. Ceci prouve (i).

Pour (ii). Soit Ω_a la clôture algébrique de K contenue dans Ω. L'inclusion $L \subset \Omega'$ se prolonge en un L-homomorphisme $\sigma : \Omega_a \to \Omega'$. On vérifie que $\sigma(N)$ est une extension normale de L dans Ω', donc $N' \subset \sigma(N)$, d'autre part $\sigma^{-1}(N')$ est aussi une extension normale de L, dans Ω, donc $N \subset \sigma^{-1}(N')$. □

Définition 2.3.2. Soient L/K une extension algébrique et Ω une extension algébriquement close de K contenant L. Le plus petit sous-corps N de Ω contenant L et normal sur K, mis en évidence en 2.3.1, s'appelle la fermeture normale de L/K dans Ω.

Remarque 2.3.3. Soient K un corps et Ω une extension algébriquement close de K. Un sous-corps de Ω extension de K engendré par *des* racines d'une famille de polynômes irréductibles sur K admet pour fermeture normale dans Ω l'extension de K engendrée par *toutes* les racines de ces polynômes. Cela se dit plus précisément de la manière suivante. Soit $(P_i)_{i\in I}$ une famille d'éléments *irréductibles* de $K[X]$ et désignons par R_i l'ensemble des racines de P_i dans Ω, $i \in I$. Soit A une partie de $\cup_{i\in I} R_i$ rencontrant chacun des R_i et posons $L = K(A)$. Alors la fermeture normale de L/K dans Ω est $N = K(\cup_{i\in I} R_i)$. Cela se voit avec l'assertion (iii) de 2.1.4 (voir aussi la définition 2.2.1).

Par exemple, la fermeture normale de l'extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ dans $\mathbb{C}$ est $N = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.

2.4 Exercices

Exercice 2.2. Soient K un corps et $P(X) \in K[X]$ de degré $n \geq 1$. Soit L un corps de décomposition de P sur K. Montrer que $[L : K]$ divise $n!$. (**Remarque.** Il est plus facile de montrer que $[L : K] \leq n!$.)

Exercice 2.3. Montrer qu'une extension de degré deux est normale.

Exercice 2.4. On considère le polynôme $P(X) = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$.

1) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$.

2) Décomposer $P(X)$ en produit de polynômes de second degré dans $\mathbb{Q}(i)$.

3) Montrer que le corps de décomposition de $P(X)$ dans $\mathbb{C}$ est $K = \mathbb{Q}(i + \sqrt{2})$.

4) On note G le groupe des $\mathbb{Q}$-automorphismes de K.

i) Quel est l'ordre de G ?

ii) Montrer qu'il existe $\varphi \in G \setminus \{id_K\}$ laissant invariant chaque élément de $\mathbb{Q}(i)$. Quel est l'ordre de φ.

iii) Montrer qu'il existe $\psi \in G \setminus \{id_K\}$ laissant invariant chaque élément de $\mathbb{Q}(\sqrt{2})$. Quel est l'ordre de ψ.

iv) Montrer que $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 2.5. 1) Soient K un corps, $f \in K[X]$, $p = \deg(f)$ un nombre premier. Supposons que, pour toute extension L de K, si f a une racine dans L, alors f se décompose en produit de facteurs de degré 1 dans $L[X]$. Montrer que f est irréductible dans $K[X]$ ou f a une racine dans K.

2) Montrer que les hypothèses de 1) sont vérifiées dans les cas suivants :

i) $f(X) = X^p - a$, $\mathrm{car}(K) = p$, $a \in K$.

ii) $f(X) = X^p - X - a$, $\mathrm{car}(K) = p$, $a \in K$.

iii) $f(X) = X^p - a$, $\mathrm{car}(K) \neq p$, $a \in K$, et K contient un élément ξ tel que $\xi^p = 1, \xi \neq 1$.

Exercice 2.6. Soit p un nombre premier. Montrer que $X^p - X + 1$ est un polynôme irréductible sur $\mathbb{F}_p$ et que son corps de décomposition est une extension (séparable) de $\mathbb{F}_p$ de degré p.

Exercice 2.7. Soit L une extension algébrique d'un corps K.

1) Soit L/K une extension normale. Soient $f \in K[X]$ irréductible et $g, h \in L[X]$ deux facteurs unitaires irréductibles de f. Montrer qu'il existe un K-automorphisme σ de L tel que $\sigma(g) = h$.

2) Donner un contre exemple quand L/K n'est pas normale.

3) Montrer que L est une extension normale de K si et seulement si, pour tout $f \in K[X]$ irréductible, les facteurs irréductibles de f dans $L[X]$ sont de même degré.

Exercice 2.8. Soit $F = \mathbb{Q}(\sqrt{2}i, \sqrt[4]{2}(1-i))$.

1) Calculer $[\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{2}i, \sqrt[4]{2}(1-i)) : \mathbb{Q}(\sqrt{2}i)]$. Ces extensions sont-elles normales ?

2) On se propose de savoir si $F/\mathbb{Q}$ est normale.

i) Montrer que $P(X) = X^4 + 8$ est irréductible dans $\mathbb{Q}[X]$.

ii) Factoriser $P(X)$ dans $\mathbb{C}[X]$.

iii) En calculant, pour u racine de $P(X)$, $\bar{u}/u$ et $(\bar{u}-u)/2i$, montrer que le corps de décomposition de $P(X)$ dans $\mathbb{C}$ est $E = \mathbb{Q}(\sqrt[4]{2}, i)$.

iv) Calculer $[E : \mathbb{Q}]$ et conclure.

Exercice 2.9. Pour chacun des polynômes $f \in K[X]$ suivants, on note E un corps de décomposition de f sur K. Déterminer $[E : K]$ et le nombre des K-automorphisme de E.

1) $K = \mathbb{Z}/3\mathbb{Z}$ et $f(X) = X^3 + 2X + 1$.

2) $K = \mathbb{Z}/p\mathbb{Z}$ et $f(X) = X^{p^8} - 1$.

3) $K = \mathrm{Fr}(\mathbb{Z}/3\mathbb{Z}[T])$ et $f(X) = X^3 - T$.

Exercice 2.10. Soit N la fermeture normale de $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ sur $\mathbb{Q}$ contenue dans $\mathbb{C}$.

1) Déterminer N et calculer $[N : \mathbb{Q}]$.

2) Montrer que $N/\mathbb{Q}(\sqrt{2})$ est normale. Déterminer tous les $\mathbb{Q}(\sqrt{2})$-automorphismes de N ainsi que l'ordre de chacun d'entre eux.

Chapitre 3

Séparabilité et inséparabilité

3.1 Le degré de séparabilité

Théorème 3.1.1. *Soit L/K une extension algébrique et soient $\sigma : K \to E$, $\tau : K \to F$ des morphismes de K dans deux corps algébriquement clos. Soient S_σ et S_τ l'ensemble des prolongements respectivement de σ et de τ à L. Alors S_σ et S_τ sont en bijection. Il suit que le cardinal de S_σ ne dépend que de l'extension L/K, il ne dépend pas du corps algébriquement clos E choisi pour l'évaluer.*

Démonstration. On peut supposer que E (resp. F) est une clôture algébrique de $\sigma(L)$ (resp. $\tau(L)$). En effet, E (resp. F) contient une clôture algébrique de $\sigma(L)$ (resp. $\tau(L)$) et les prolongements de σ (resp. τ) arrivent dans cette clôture algébrique. Soit

$$\sigma(K) \xrightarrow{\sigma^{-1}} K \xrightarrow{\tau} F$$

et soit $u : E \to F$ un prolongement de cette application à E. On a $u(E) = F$ car $u(E)$ est inclus dans F et est algébriquement clos. Ceci permet de définir l'application $S_\sigma \to S_\tau$ qui à α associe $u \circ \alpha$, ainsi que son application réciproque, qui à $\beta \in S_\tau$ associe $u^{-1} \circ \beta$. D'où l'égalité des cardinaux. □

Remarque 3.1.2. Soient L/K une extension algébrique, $\sigma : K \to E$ un morphisme de K dans un corps algébriquement clos E et S_σ l'ensemble des prolongements σ à L, il résulte de 1.5.8 que S_σ est non vide.

Définition 3.1.3. Soit L/K une extension algébrique et soit $\sigma : K \to E$ un morphisme de K dans un corps algébriquement clos. Soit S_σ l'ensemble des prolongements de σ à L. Alors le cardinal de S_σ se note $[L : K]_s$ et s'appelle le degré de séparabilité de L sur K.

Proposition 3.1.4. *Soient $K \subset L \subset E$ des extensions algébriques, alors $[E : K]_s$ est fini si et seulement si $[E : L]_s$ et $[L : K]_s$ le sont, auquel cas l'on a*

$$[E : K]_s = [E : L]_s [L : K]_s.$$

Démonstration. Soit $\sigma : K \to \Omega$ un morphisme de K dans un corps algébriquement clos Ω et soit $S_{L/K,\sigma}$ l'ensemble des prolongement de σ à L. Pour tout τ appartenant à $S_{L/K,\sigma}$, soit $S_{E/L,\tau}$ l'ensemble des prolongements de τ à E. Soit encore $S_{E/K,\sigma}$ l'ensemble des prolongements de σ à E. On a

$$S_{E/K,\sigma} = \bigcup_{\tau \in S_{L/K,\sigma}} S_{E/L,\tau}$$

et cette réunion est disjointe. Il en résulte la proposition. □

La proposition suivante donne des précisions sur le degré de séparabilité lorsque l'extension L/K est *monogène*, c'est à dire lorsque il existe $x \in L$ tel que $L = K(x)$. Elle est très utile pour les applications.

Proposition 3.1.5. *Soit $K(x)$ une extension algébrique de K engendrée par un élément.*
(i) Le degré de séparabilité $[K(x) : K]_s$ est égal au nombre de racines distinctes du polynôme $\mathrm{irr}(x, K; X)$ *(racines distinctes dans une clôture algébrique de K).*
(ii) Soit p l'exposant caractéristique de K (cf. §1.2) et soit $n \in \mathbb{N}$ l'entier ainsi défini : si $p = 1$ on a $n = 0$, si $p \geq 2$, alors n est le plus grand entier tel qu'il existe un polynôme $Q(X) \in K[X]$ vérifiant $\mathrm{irr}(x, K; X) = Q(X^{p^n})$. *Alors*

$$[K(x) : K] = p^n [K(x) : K]_s.$$

L'entier p^n ainsi défini s'appelle le degré d'inséparabilité de x sur K.

Démonstration. (i) Soit Ω un corps algébriquement clos contenant K et posons $P(X) = \mathrm{irr}(x, K; X)$. Soit $\sigma : K(x) \to \Omega$ un prolongement de l'inclusion $i : K \hookrightarrow \Omega$, alors

$$0 = \sigma(P(x)) = P(\sigma(x)),$$

donc $\sigma(x)$ est une racine de $P(X)$ dans Ω. Inversement, soit $y \in \Omega$ une racine de $P(X)$, alors (cf. 1.3.4)

$$K(x) \simeq \frac{K[X]}{(P(X))} \simeq K(y) \subset \Omega$$

est un prolongement de $i : K \hookrightarrow \Omega$ à $K(x)$.

La preuve de (ii) nécessite le lemme intermédiaire suivant.

Lemme 3.1.6. *Soient K un corps de caractéristique p et $P(X)$ un élément irréductible de $K[X]$. Soit Ω un corps algébriquement clos, extension de K.*
(i) Si $p = 0$, alors $P(X)$ n'a que des racines simples dans Ω.
(ii) Si $p \geq 2$, alors $P(X)$ a une racine multiple dans Ω si et seulement si son polynôme dérivé est le polynôme nul, auquel cas il existe $Q(X) \in K[X]$ tel que $P(X) = Q(X^p)$.

Montrons le lemme. On vérifie d'abord que $x \in \Omega$ est racine multiple (en fait double) du polynôme P si et seulement si il est racine de P et de P'. En effet si x est racine double, on écrit $P(X) = (X-x)^2 Q(X)$ dans $\Omega[X]$ et il vient $P'(X) = 2(X-x)Q(X) + (X-x)^2 Q'(X)$. Si $P(X) = (X-x)Q(X)$ dans $\Omega[X]$, on a $P'(X) = Q(X) + (X-x)Q'(X)$, ce qui implique que si x est racine de P', alors il l'est de Q.

Soit x une racine de P dans Ω. Comme P est irréductible, il existe $\lambda \in K^*$ tel que $P(X) = \lambda \mathrm{irr}(x, K; X)$. Supposons que x est racine multiple de P, alors x est racine du polynôme dérivé $\mathrm{irr}(x, K; X)'$, par suite ce dernier est divisible par $\mathrm{irr}(x, K; X)$ (cf. 1.3.2). Comme

$$\deg \mathrm{irr}(x, K; X) > \deg \mathrm{irr}(x, K; X)',$$

il vient que $\mathrm{irr}(x, K; X)' = 0$. Donc $P' = 0$. Ecrivons $P(X) = \sum_{0 \le i \le d} a_i X^i$ (avec les a_i dans K), alors la relation $P' = 0$ implique que $ia_i = 0$ pour tout i, donc $a_i = 0$ ou $i = 0$ dans K ($i = 0$ dans K signifie que l'entier i est divisible par la caractéristique p de K). Donc $P(X)$ s'écrit alors $P(X) = \sum_{0 \le i \le dp^{-1}} a_i X^{pi}$. Inversement, une telle écriture de P montre que sa dérivée est nulle, par suite que toutes ses racines sont aussi des racines de P'.

Le lemme est donc démontré, revenons à la preuve de (ii) de 3.1.5. Si la caractéristique de K est nulle, le lemme dit que le nombre de racines distinctes de $irr(x, K; X)$ est égal à son degré, d'où, avec (i) : $[K(x) : K] = [K(x) : K]_s$.

Supposons maintenant que la caractéristique de K est $p > 0$, posons $P(X) = \mathrm{irr}(x, K; X)$ et soient n, Q définis dans l'énoncé. Alors $Q' \neq 0$, car grâce au lemme, le contraire contredirait la maximalité de n. De plus, Q est un élément irréductible de $K[X]$, car toute factorisation de Q en donne une de P. Soit Ω un corps algébriquement clos, contenant x et extension de K, on écrit dans $\Omega[X]$

$$Q(X) = \lambda \prod_{1 \le i \le \delta} (X - x_i)$$

(avec $\lambda \in K$) et, comme Q est irréductible dans K et que son polynôme dérivé est non nul, les x_i sont deux à deux distincts. Pour $1 \le i \le \delta$, soit $y_i \in \Omega$ tel que $y_i^{p^n} = x_i$ (on peut remarquer que y_i est unique car dans $\Omega[X]$: $X^{p^n} - x_i = X^{p^n} - y_i^{p^n} = (X - y_i)^{p^n}$). On a

$$P(X) = Q(X^{p^n}) = \lambda \prod_{1 \le i \le \delta} (X^{p^n} - x_i) = \lambda \prod_{1 \le i \le \delta} (X^{p^n} - y_i^{p^n}) = \lambda \prod_{1 \le i \le \delta} (X - y_i)^{p^n}.$$

Ainsi les racines distinctes de P dans Ω sont les $y_1, \cdots, y_\delta$, elles sont au nombre de δ, et l'on a

$$\deg(\mathrm{irr}(x, K; X)) = \deg(P(X)) = p^n \delta = p^n [K(x) : K]_s,$$

la dernière égalité venant de (i). Ceci est la formule cherchée □

Remarque 3.1.7. Quelques propriétés importantes sont apparues dans la démonstration précédente, nous les rappelons. Soient K un corps d'exposant caractéristique p et P un élément de $K[X]$, irréductible. Soient $n \in \mathbb{N}$ et $Q \in K[X]$ donnés par la proposition 3.1.5. Alors $P(X) = Q(X^{p^n})$, le polynôme dérivé de Q étant non nul, ou, ce qui revient au même, le polynôme Q n'ayant dans une (ou dans toute) clôture algébrique K^{alg} de K que des racines simples (on dira, avec la définition suivante, qu'un tel polynôme est *séparable*). De plus si $x_1, \cdots, x_\delta$ sont les racines de Q dans K^{alg}, si $y_1, \cdots, y_\delta$ sont des éléments de K^{alg} tels que $y_i^{p^n} = x_i$, alors les y_i, $1 \leq i \leq \delta$, sont les racines distinctes de P, toutes de même multiplicité p^n (rappelons que P est irréductible dans $K[X]$ et que les notations sont celles de 3.1.5).

Définition 3.1.8. Soient K un corps et P un polynôme à coefficient dans K. On dit que P est séparable si, dans une clôture algébrique de K, P n'a que des racines simples. Il revient au même de dire que P n'a que des racines simples dans toute clôture algébrique de K, ou encore, lorsque P est irréductible dans $K[X]$, que le polynôme dérivé de P est non nul.

Exemple 3.1.9. (i) Soient K un *corps de caractéristique* 0, il suit de 3.1.5 que tous les éléments *irréductibles* de $K[X]$ sont des polynômes séparables.
(ii) Soient p un nombre premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $K = \mathbb{F}_p(T)$. Soit $P(X) = X^{p^2} + TX^p + T \in K[X]$. Alors $P(X)$ est irréductible dans $K[X]$ et l'on a $P(X) = Q(X^p)$ où $Q(X) = X^p + TX + T \in K[X]$. On vérifie que $Q'(X) = T \neq 0$.

3.2 Les extensions séparables

Définition 3.2.1. Soit L/K une extension algébrique.
(i) Soit x appartenant à L. On dit que x est séparable sur K si

$$[K(x) : K] = [K(x) : K]_s.$$

(ii) On dit que L est séparable sur K, ou que l'extension L/K est séparable, si tout élément de L est séparable sur K. Sinon, on dit que L est inséparable sur K, que l'extension L/K est inséparable ou encore qu'elle possède de l'inséparabilité.

Remarque 3.2.2. Soit L/K une extension algébrique et soit x appartenant à L, il résulte de 3.1.5 (voir aussi 3.1.7 et 3.1.8) que x est séparable sur K si et seulement si $\mathrm{irr}(x, K; X)$ est un polynôme séparable. Ceci montre que lorsque K est de *caractéristique* 0*, toutes ses extensions algébriques sont séparables* (cf. (i) de 3.1.9).

La proposition suivante donne des propriétés importantes des extensions séparables.

Proposition 3.2.3. *(i) Soit L/K soit une extension algébrique finie et soit p l'exposant caractéristique de K, alors il existe $n \in \mathbb{N}$ tel que*

$$[L : K] = p^n [L : K]_s,$$

avec $n = 0$ si $p = 1$. Cet entier p^n s'appelle le degré d'inséparabilité de L sur K.
(ii) Soit L/K une extension algébrique finie, elle est séparable si et seulement si

$$[L : K] = [L : K]_s.$$

(iii) Soit L/K une extension et soit M une partie de L formée d'éléments algébriques et séparables sur K, alors $K(M)$ est une extension séparable de K.
(iv) Soient $K \subset L \subset E$ des extensions algébriques, alors E/K est séparable si et seulement si il en est de même des deux extensions E/L et L/K.

Démonstration. (i) On écrit $L = K(x_1, \cdots, x_r)$. Posons $K_0 = K$ et $K_i = K(x_1, \cdots, x_i)$ pour $1 \leq i \leq r$. L'extension L/K se décompose en la suite d'extensions

$$K_0 \subset K_1 \subset \cdots \subset K_r.$$

Pour $1 \leq i \leq r$ soit p^{n_i} le degré d'inséparabilité de x_i sur K_{i-1} (cf. 3.1.5), on a

$$[K_{i-1} : K_i] = p^{n_i} [K_{i-1} : K_i]_s.$$

Il suit des deux formules précédentes, de la propriété 1.1.5 de multiplicité des degrés et de celle 3.1.4 des degrés de séparabilité, que l'on a

$$[L : K] = p^{n_1 + \cdots + n_r} [L : K]_s.$$

(ii) Supposons L/K séparable et reprenons les notations de la preuve de (i). Par hypothèse, l'élément x_i de L est séparable sur K, donc sur K_{i-1}, puisque $\mathrm{irr}(x_i, K_{i-1}; X)$ est un diviseur dans $K_{i-1}[X]$ de $\mathrm{irr}(x_i, K; X)$ (ce dernier n'a que des racines simples dans toute clôture algébrique de K), on a donc $n_i = 1$ pour tout i, par suite $[L : K] = [L : K]_s$.

Supposons $[L : K] = [L : K]_s$, soit $x \in L$. Soient p^m et p^n les degrés d'inséparabilité de L sur $K(x)$ et de $K(x)$ sur K, on a,

$$[L : K]_s = [L : K] = [L : K(x)][K(x) : K]$$

$$= p^n [L : K(x)]_s p^m [K(x) : K]_s = p^{n+m} [L : K]_s,$$

donc $m = 0$, c'est à dire $[K(x) : K] = [K(x) : K]_s$.

(iii) Soit $x \in K(M)$, alors il existe des éléments $x_1, \cdots, x_r$ de M, en nombre fini, tels que $x \in K(x_1, \cdots, x_r)$ (cf. 1.1.9). Posons $K_0 = K$ et $K_i = K(x_1, \cdots, x_i)$ pour $1 \leq i \leq r$. Montrons que $[K_r : K] = [K_r : K]_s$, il en résultera avec (ii) que x est séparable sur K. Les arguments pour montrer

cette égalité sont proches de ceux utilisés lors de la preuve de (ii). Soit p^{n_i} le degré d'inséparabilité de x_i sur K_{i-1}, par hypothèse, x_i est séparable sur K, donc sur K_{i-1}, puisque $\mathrm{irr}(x_i, K_{i-1}; X)$ est un diviseur dans $K_{i-1}[X]$ de $\mathrm{irr}(x_i, K; X)$, il suit $n_i = 0$ pour tout i, donc (propriété de multiplicité des degrés et des degrés de séparabilité) $[K_r : K] = [K_r : K]_s$.
(iv) Supposons E/K séparable. Soit $x \in E$, alors on voit que $\mathrm{irr}(x, L; X)$ est séparable (toujours avec le même argument : puisque x est séparable sur K et que $\mathrm{irr}(x, L; X)$ divise dans $L[X]$ le polynôme $\mathrm{irr}(x, K; X)$, ce dernier étant séparable). Soit $x \in L$, alors x est séparable sur K puisque c'est un élément de E.

Supposons que E/L et L/K sont séparables. Soit $x \in E$, posons

$$P(X) = \mathrm{irr}(x, L; X) = X^d + a_1 X^{d-1} + \cdots + a_d$$

avec donc $a_1, \cdots, a_d$ dans L. Considérons les extensions

$$K \subset K(a_1, \cdots, a_d) \subset K(x, a_1, \cdots, a_d),$$

ce sont des extensions algébriques finies. Comme les a_i sont séparables sur K, il vient avec (iii) que la première extension est séparable. Le polynôme irréductible de x sur $K(a_1, \cdots, a_d)$ divise $P(X)$ (puisque ce dernier est à coefficients dans $K(a_1, \cdots, a_d)$), il est donc séparable et la deuxième extension est aussi séparable. La propriété de multiplicité des degrés et des degrés de séparabilité permet de conclure. □

Dans le théorème suivant, on décompose les extensions algébriques en faisant apparaître une classe d'extensions, qui est l'objet d'étude du prochain paragraphe.

Théorème 3.2.4. *Soit L/K une extension algébrique, alors il existe un unique sous corps de L, noté L_s, intermédiaire entre K et L, maximal parmi les extensions séparables de K contenues dans L. L'extension L_s/K s'appelle la sous-extension séparable maximale de L/K. On a*

$$[L : L_s]_s = 1,$$

(on dit que l'extension L_s/L est purement inséparable). Supposons $[L : K]_s$ fini, alors on a

$$[L : K]_s = [L_s : K] = [L_s : K]_s.$$

Démonstration. Soit M l'ensemble des éléments de L séparables sur K et posons $L_s = K(M)$, d'après (iii) de 3.2.3 l'extension L_s/K est séparable et sa définition montre qu'elle est maximale.

Montrons $[L : L_s] = 1$. Soit y un élément de L. Soit p^n le degré d'inséparabilité de y sur L_s (donc p est la caractéristique de K), c'est à dire que l'on a

$$\mathrm{irr}(y, L_s; X) = Q(X^{p^n})$$

avec $Q(X) \in L_s[X]$, irréductible et séparable, en particulier

$$Q(X) = \mathrm{irr}(y^{p^n}, L_s; X).$$

Il résulte de ceci que y^{p^n} est séparable sur L_s, par suite sur K (cf. (iv) de 3.2.3). Il vient alors, par définition de L_s, que y^{p^n} appartient à L_s (donc que $\deg Q = 1$).

Considérons un corps algébriquement clos contenant L, par exemple une clôture algébrique L^{alg} de L. Soit $i : L_s \hookrightarrow L^{\mathrm{alg}}$ l'inclusion et

$$\sigma \ : L \longrightarrow L^{\mathrm{alg}}$$

un prolongement de i à L. On a $\sigma(y^{p^n}) = \sigma(y^{p^n}$ puisque $(y^{p^n} \in L_s$. Il en résulte $\sigma(y) = y$. On a prouvé ainsi que l'inclusion $i : L_s \hookrightarrow L^{\mathrm{alg}}$ admet un unique prolongement à $L_s(y)$ (qui est encore l'inclusion) pour tout $y \in L$, ceci montre que L/L_s est purement inséparable.

La deuxième formule du théorème découle de ce qui précède. Soient $\alpha : K \to \Omega$ un morphisme dans un corps algébriquement clos, $\beta : L_s \to \Omega$ un prolongement de α, alors il n'y a qu'un seul prolongement de β à L, puisque $[L : L_s] = 1$. De plus L_s/K étant séparable, on a que $[L_s : K] = [L_s : K]_s$ lorsque ces nombres sont finis. □

Remarque 3.2.5. Soit $\alpha : K \to \Omega$ un morphisme de corps, Ω étant algébriquement clos , soient $K \subset E \subset L$ deux extensions algébriques. Notons $\mathrm{Hom}_\alpha(E, \Omega)$ et $\mathrm{Hom}_\alpha(L, \Omega)$ les ensembles des prolongements de α à E et L respectivement. Alors, d'après 1.5.8, la restriction de L à E induit une application surjective

$$\mathrm{Hom}_\alpha(L, \Omega) \longrightarrow \mathrm{Hom}_\alpha(E, \Omega).$$

Lorsque $[L : E]_s = 1$, c'est à dire lorsque l'extension L/E est purement inséparable (selon le vocabulaire précisé au paragraphe suivant), cette application est de plus injective. Nous avons utilisé cet argument au dessus pour $E = L_s$.

La remarque suivante est très utile pour les applications concrètes.

Remarque 3.2.6. Soit $K(x)/K$ une extension algébrique monogène (c'est à dire engendrée par un seul élément). Soit p^n le degré d'inséparabilité de x sur K (donc p est la caractéristique de K), on peut écrire

$$\mathrm{irr}(x, K; X) = Q(X^{p^n}),$$

où $Q(X) \in K[X]$ est irréductible et séparable, en particulier

$$Q(X) = \mathrm{irr}(x^{p^n}, K; X).$$

Examinons les extensions

$$K \subset K(x^{p^n}) \subset K(x),$$

La première extension est séparable puisque $Q(X)$ est un polynôme séparable, d'autre part l'examen des degrés montre que

$$\mathrm{irr}(x, K(x^{p^n}); X) = X^{p^n} - x^{p^n},$$

en particulier $[K(x) : K(x^{p^n})]_s = 1$ (l'extension $K(x)/K(x^{p^n})$ est purement inséparable). Il vient donc

$$K(x)_s = K(x^{p^n}),$$

où p^n est le degré d'inséparabilité de x sur K.

Soit L/K une extension algébrique et pour tout $x \in L$ soit p^{n_x} le degré d'inséparabilité de x sur K (donc, ici aussi, p désigne la caractéristique de K). On montre, avec les mêmes arguments que précédemment, que

$$L_s = K(\{x^{p^{n_x}} \ / \ x \in L\}).$$

3.3 Les extensions purement inséparables

Définition 3.3.1. Soit L/K une extension algébrique.
(i) On dit qu'un élément x de L est purement inséparable sur K si $[K(x) : K]_s = 1$.
(ii) On dit que L est purement inséparable sur K, ou que l'extension L/K est purement inséparable, si tout élément de L est purement inséparable sur K.

Proposition 3.3.2. *(i) Soit L/K une extension algébrique, alors elle est purement inséparable si et seulement si*

$$[L : K]_s = 1.$$

(ii) Soit L/K une extension algébrique et soit M une partie de L formée d'éléments purement inséparables sur K, alors $K(M)/K$ est une extension purement inséparable.
(iii) Soient $K \subset L \subset E$ deux extensions algébriques, alors E/K est purement inséparable si et seulement si les deux extensions E/L et L/K le sont.

Démonstration. (i) Supposons $[L : K]_s = 1$. Soit $x \in L$. Alors, la propriété 3.1.4 de multiplicité des degrés de séparabilité montre

$$1 = [L : K]_s = [L : K(x)]_s [K(x) : K]_s,$$

donc $[K(x) : K]_s = 1$. Inversement, supposons que tout élément de L est purement inséparable sur K. Soient $\alpha : K \to \Omega$ un morphisme de K dans un corps Ω algébriquement clos, $\beta, \gamma : L \to \Omega$ deux prolongements de α à L. Si β et γ sont distincts, il existe $x \in L$ tel que $\beta(x) \neq \gamma(x)$, mais alors

les restrictions de β et γ à $K(x)$ contredisent la relation $[K(x) : K]_s = 1$. Il vient $\beta = \gamma$, finalement $[L : K]_s = 1$.

(ii) Soit $\alpha : K \to \Omega$ un morphisme de K dans un corps algébriquement clos Ω et supposons que α possède deux prolongements distincts, β et γ, à $K(M)$. Ainsi il existe $x \in M$ tel que $\beta(x) \neq \gamma(x)$, mais alors les restrictions de β et γ à $K(x)$ contredisent le fait que x est purement inséparable sur K.

(iii) C'est une conséquence immédiate de la propriété 3.1.4 de multiplicité des degrés de séparabilité. □

Remarque 3.3.3. Soient K un corps de caractéristique $p > 0$ et L/K une extension algébrique finie.
(i) Supposons L/K purement inséparable, alors il résulte de 3.2.3 que le degré de cette extension est une puissance de p.
(ii) Il ne faut surtout pas déduire de ce qui précède que si l'extension L/K est séparable, alors son degré n'est pas divisible par p. Par exemple, soient $K = \mathbb{Z}/p\mathbb{Z}(T)$, un corps de fractions rationnelles à une indéterminées et à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, $P(X) = X^p + T^2X + T \in K[X]$. Le polynôme $P(X)$ est irréductible sur K, n'importe laquelle de ses racines (dans une clôture algébrique de K) engendre sur K une extension séparable de degré p.

3.4 Séparabilité et normalité

Le lemme suivant est presque une évidence, mais le phénomène qu'il précise est suffisamment important pour être mis en exergue.

Lemme 3.4.1. *Soient L/K une extension finie et normale et $G = \mathrm{Gal}(L/K)$ (cf. 2.2.4). Alors on a*

$$[L : K]_s = o(G),$$

où $o(G)$ désigne l'ordre de G.

Démonstration. En effet, soit Ω un corps algébriquement clos admettant L comme sous-corps, alors tout K-homomorphisme de L dans Ω est un K-automorphisme de L. □

Selon les notations habituelles, étant donné un groupe G agissant sur un corps L, on pose

$$L^G = \{x \in L \ / \ g(x) = x \ \forall g \in G\}.$$

Théorème 3.4.2. *Soit L/K une extension normale et soit $G = \mathrm{Gal}(L/K)$. (i) L'extension L^G/K est purement inséparable, l'extension L/L^G est séparable et normale (à partir du chapitre suivant on appellera "galoisiennes" les extensions séparables et normales), on a*

$$\mathrm{Gal}(L/L^G) = G.$$

(ii) Supposons l'extension L/K finie, alors

$$[L : L^G] = [L : K]_s = o(G),\ [L^G : K] = \textit{degré d'inséparabilité de } L/K.$$

(iii) On a (cf. 3.2.4)

$$L_s \cap L^G = K \quad , \quad L_s \cdot L^G = L,$$

ce dernier étant le compositum de L_s et L^G dans L.

Démonstration. (i) Soit Ω un corps algébriquement clos admettant L comme sous-corps, alors tout K-homomorphisme de L^G dans Ω se prolonge en un K-automorphisme de L, donc est l'identité sur L^G. Ceci prouve que $[L^G : K]_s = 1$.

Montrons que L/L^G est séparable. Soit $x \in L$ et, dans L, soient $x = x_1, \cdots, x_d$ les racines *distinctes* de $\mathrm{irr}(x, K; X)$. Les fonctions symétriques des racines (qui permettent d'exprimer les coefficients des polynômes) montrent que

$$Q(X) = \prod_{1 \le i \le d} (X - x_i)$$

à ses coefficients stables sous l'action de G, ils sont donc dans L^G. Ainsi $\mathrm{irr}(x, L^G; X)$ divise $Q(X)$ et ce dernier est séparable, donc x est séparable sur L^G. Par suite L/L^G est séparable, elle est normale en vertu de l'assertion (i) de 2.2.2, l'égalité des groupes de Galois vient du fait que tout K-automorphisme de L est trivial sur L^G.

(ii) C'est une conséquence directe de la propriété de multiplicité des degrés et des degrés de séparabilité ainsi que du lemme 3.4.1.

(iii) L'extension $L_s \cap L^G$ de K est séparable car c'est un sous-extension de L_s/K, purement inséparable car c'est une sous-extension de L^G/K, elle est donc égale à K.

Le corps L est une extension de $L_s \cdot L^G$ qui est d'une part séparable, puisque c'est une sous-extension de L/L^G, d'autre part purement inséparable, car c'est une sous-extension de L/L_s, d'où l'égalité cherchée. □

3.5 Les corps parfaits

Définition 3.5.1. Un corps est dit parfait si toutes ses extensions algébriques sont séparables.

Les corps algébriquement clos et les corps de caractéristique nulle sont parfaits. Le théorème suivant implique qu'il en est de même des corps finis.

Définition 3.5.2. Soit K un corps de caractéristique $p > 0$. On appelle endomorphisme absolu de Frobenius de K l'endomorphisme F de K qui à x associe x^p.

Théorème 3.5.3. *Soit K un corps de caractéristique $p > 0$, alors K est parfait si et seulement si son endomorphisme absolu de Frobenius est un automorphisme.*

Démonstration. Soit F l'endomorphisme absolu de Frobenius de K. Supposons K parfait, il faut prouver que F est surjectif. Soit $x \in K$ et, dans une clôture algébrique K^{alg} de K, soit y une racine du polynôme $X^p - x$. Alors dans $K[X]$ le polynôme $\mathrm{irr}(y, K; X)$ divise $X^p - x$, et ce dernier a une seule racine, qui est y, dans K^{alg}. On voit que y est purement inséparable sur K, donc $y \in K$. Ainsi x possède un antécédant par F.

Supposons que F est un automorphisme. Il suffit de montrer que toute extension finie L/K est séparable. Soient donc L/K une extension finie, N sa fermeture normale dans une clôture algébrique fixée de K (cf. 2.3.2)) et $G = \mathrm{Gal}(N/K)$. La propriété 3.4.2 ainsi que celle de multiplicité des degrés et degrés de séparabilité montrent que si $N^G = K$ alors L/K est séparable.

Montrons $N^G = K$. Soit $x \in N^G$, alors x est purement inséparable sur K, soit p^n son degré sur K et supposons que x n'est pas dans K, c'est à dire $n > 0$. Posons $y = x^{p^{n-1}}$, c'est un élément de N^G de degré p sur K, par conséquent $y^p \in K$. Comme F est surjectif, il existe $z \in K$ tel que $F(z) = y^p$, ce qui s'écrit $z^p = y^p$, on a donc $z = y$, par suite $y \in K$. Ceci contredit le fait que $x \notin K$. □

Corollaire 3.5.4. *Les corps finis sont parfaits.*

Démonstration. En effet, comme l'endomorphisme F est une application injective d'un ensemble fini dans lui-même, il est aussi surjectif. □

3.6 Les extensions monogènes

On a déjà rencontré cette notion, rappelons en la définition.

Définition 3.6.1. Soit L/K une extension, on dit qu'elle est monogène s'il existe un élément x de L tel que $L = K(x)$. Un tel x est dit élément primitif de L sur K.

Théorème 3.6.2. *Soit L/K une extension finie, alors elle est monogène si et seulement si elle ne possède qu'un nombre fini de sous-extensions.*

Démonstration. Supposons que K est un corps fini, alors L est aussi un corps fini, donc le groupe multiplicatif L^* est cyclique [1]. Soit x un générateur de L^*, clairement $L = K(x)$. On suppose maintenant que K est infini.

Supposons L/K monogène, $L = K(x)$. Soit E un corps intermédiaire entre K et $K(x)$ (donc $K \subset E \subset K(x)$). Posons

$$\mathrm{irr}(x, E; X) = X^d + a_1 X^{d-1} + \cdots + a_d.$$

[1] Nous supposons ce résultat connu, même si nous allons le redémontrer dans le chapitre sur les corps finis.

On a

$$K(a_1, \cdots, a_d) \subset E \quad , \quad [L : E] = d$$

et aussi

$$[L : K(a_1, \cdots, a_d)] \leq d$$

puisque $\mathrm{irr}(x, E : X)$ est à coefficients dans $K(a_1, \cdots, a_d)$. Il en résulte que

$$E = K(a_1, \cdots, a_d).$$

On voit que E est déterminé par les coefficients de $\mathrm{irr}(x, E; X)$, on peut remarquer que ce dernier est un diviseur de $\mathrm{irr}(x, K; X)$ dans $K(x)[X]$. Les sous-extensions de L/K sont donc déterminées par les coefficients des diviseurs de $\mathrm{irr}(x, K; X)$ dans $K(x)[X]$, ces derniers sont en nombre finis.

Inversement, supposons que les sous-extensions de L/K sont en nombre fini. On pose $L = K(x_1, \cdots, x_r)$, considérons la suite d'extensions

$$K \subset K(x_1) \subset K(x_1, x_2) \subset \cdots \subset K(x_1, \cdots, x_i) \subset \cdots \subset K(x_1, \cdots, x_r).$$

Par récurrence sur i, on voit qu'il suffit de montrer le résultat pour $L = K(x_1, x_2)$, ce que nous faisons. Considérons les corps $K(x_1 + \lambda x_2)$, pour $\lambda \in K$. Par hypothèse ils sont en nombre fini, donc, puisque K est infini, il existe λ et μ appartenant à K, $\lambda \neq \mu$, tels que

$$K(x_1 + \lambda x_2) = K(x_1 + \mu x_2).$$

On a donc

$$x_1 + \lambda x_2 \ , \ x_1 + \mu x_2 \in K(x_1 + \lambda x_2),$$

par suite

$$(x_1 + \lambda x_2) - (x_1 + \mu x_2) = (\lambda - \mu) x_2 \in K(x_1 + \lambda x_2),$$

dont il résulte que x_2, puis x_1, sont dans $K(x_1 + \lambda x_2)$. On a prouvé

$$K(x_1, x_2) = K(x_1 + \lambda x_2).$$

□

Corollaire 3.6.3. *(Théorème de l'élément primitif.) Soit L/K une extension séparable finie, alors elle est monogène.*

Démonstration. Soit Ω un corps algébriquement clos extension de L, on va montrer que l'application qui à E associe $\mathrm{Hom}_E(L, \Omega)$ est une injection définie sur l'ensemble des corps intermédiaires entre K et L, à valeurs dans l'ensemble des parties de $\mathrm{Hom}_K(L, \Omega)$. Il en résultera que l'ensemble des sous-extensions de L/K est fini, donc, suivant 3.6.2, que l'extension L/K est monogène.

Soient E_1 et E_2, deux corps intermédiaires entre K et L, tels que

$$(1) \quad \mathrm{Hom}_{E_1}(L,\Omega) = \mathrm{Hom}_{E_2}(L,\Omega).$$

Soit E le compositum dans L de E_1 et E_2. Le fait que L/K soit séparable implique qu'il en est de même pour toutes les extensions intermédiaires, donc

$$(2) \quad [L:E] = \mathrm{card}(\mathrm{Hom}_E(L,\Omega)) \ \leq \ [L:E_1] = \mathrm{card}(\mathrm{Hom}_{E_1}(L,\Omega)),$$

l'inégalité venant de ce que $E_1 \subset E$. Il résulte d'autre part de (1) que

$$(3) \quad \mathrm{Hom}_{E_1}(L,\Omega) \subset \mathrm{Hom}_E(L,\Omega).$$

Les relations (2) et (3) impliquent $E = E_1$, donc $E_1 = E_2$. □

Remarque 3.6.4. Soit $L = K(x_1, x_2)$ une extension séparable finie de K, une méthode concrète pour trouver un générateur de cette extension (c'est à dire trouver $x \in L$ tel que $L = K(x)$) est la suivante. Soit Ω un corps algébriquement clos extension de L. Il s'agit de trouver $\lambda \in K$ tel que pour tout $\sigma \in \mathrm{Hom}_K(L,\Omega)$ on ait

$$\sigma(x_1 + \lambda x_2) \neq x_1 + \lambda x_2.$$

En effet cette relation est équivalente au fait que

$$\mathrm{card}(\{\sigma(x_1 + \lambda x_2) \ / \ \sigma \in \mathrm{Hom}_K(L,\Omega)\}) = [L:K],$$

qui montre que le nombre de racines distinctes de $\mathrm{irr}(x_1 + \lambda x_2, K; X)$ est au moins $[L:K]$, donc que

$$[L:K] \leq [K(x_1 + \lambda x_2) : K]_s = [K(x_1 + \lambda x_2) : K]$$

(cf. 3.1.5). Comme $K(x_1 + \lambda x_2) \subset L$, il en résulte $K(x_1 + \lambda x_2) = L$.

Exercice 3.1. Montrer que l'extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ est normale. Déterminer $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[4]{2}), \mathbb{C})$, puis $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$. En déduire que $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2} + i)$.

3.7 La norme et la trace

Définition 3.7.1. Soient L/K une extension séparable finie, K^{alg} une clôture algébrique de K et posons $H_{L/K} = \mathrm{Hom}_K(L, K^{\mathrm{alg}})$. Pour tout élément x de L soient

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in H_{L/K}} \sigma(x),$$

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in H_{L/K}} \sigma(x),$$

appelés respectivement la norme et la trace de L sur K de l'élément x de L.

Théorème 3.7.2. *Soit L/K une extension séparable finie.*
(i) Soit x un élément de L, écrivons

$$\mathrm{irr}(x,K;X) = X^d + a_1X^{d-1} + \cdots + a_d$$

avec donc $a_i \in K$ pour $1 \leq i \leq d$. On a

$$\mathrm{N}_{K(x)/K}(x) = (-1)^d a_d \quad et \quad \mathrm{Tr}_{K(x)/K}(x) = -a_1.$$

(ii) $\mathrm{N}_{L/K}$ et $\mathrm{Tr}_{L/K}$ sont des applications à valeurs dans K, elles ne dépendent pas du choix de la clôture algébrique de K utilisée dans leurs définitions,

$$\mathrm{N}_{L/K} : L^* \longrightarrow K^*$$

est un homomorphisme de groupes multiplicatifs et

$$\mathrm{Tr}_{L/K} : L \longrightarrow K$$

est un homomorphisme de groupes additifs.
(iii) Soit E un corps intermédiaire entre K et L (on a donc $K \subset E \subset L$), alors

$$\mathrm{N}_{L/K} = \mathrm{N}_{E/K} \circ \mathrm{N}_{L/E} \quad et \quad \mathrm{Tr}_{L/K} = \mathrm{Tr}_{E/K} \circ \mathrm{Tr}_{L/E}.$$

Démonstration. (i) Soit K^{alg} une clôture algébrique de K et posons $H_{K(x)/K} = \mathrm{Hom}_K(K(x), K^{\mathrm{alg}})$. On a dans $K^{\mathrm{alg}}[X]$

$$\mathrm{irr}(x,K;X) = X^d + a_1X^{d-1} + \cdots + a_d = \prod_{\sigma \in H_{K(x)/K}} (X - \sigma(x)),$$

d'où les formules cherchées.

Soit E un corps intermédiaire entre K et L, posons

$$H_{E/K} = \mathrm{Hom}_K(E, K^{\mathrm{alg}}) = \{\sigma_1, \cdots, \sigma_d\}$$

et $\delta = [L : E]$. Pour tout i, $1 \leq i \leq d$, soit

$$\{\tau_{i,j} \ / \ 1 \leq j \leq \delta\}$$

l'ensemble des prolongements de σ_i à L (ils sont au nombre de δ car L/E est séparable).

Montrons (ii). Soit x un élément de L, utilisons les notations précédentes pour $E = K(x)$. Dans K^{alg} on a $\tau_{i,j}(x) = \sigma_i(x)$ pour tous i et j, donc

$$\mathrm{N}_{L/K}(x) = \prod_{1 \leq i \leq d, 1 \leq j \leq \delta} \tau_{i,j}(x) = \prod_{1 \leq i \leq d} \sigma_i(x)^\delta = \mathrm{N}_{K(x)/K}(x)^\delta.$$

Le même raisonnement, en remplaçant les produits par des sommes, montre aussi que

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{K(x)/K}(x)^\delta.$$

Avec (i) ceci prouve que la norme et la trace ne dépendent pas du choix de K^{alg}, le fait que ce soit des homomorphismes est une conséquence directe de leurs définitions.

Montrons (iii). D'après (ii), on peut supposer que K^{alg} contient E, quitte à le remplacer par une clôture algébrique de E. Nous énonçons l'assertion suivante sous forme de lemme, car elle est très utile dans les applications.

Lemme 3.7.3. *Soient $K \subset E \subset L$ des extensions finies et séparables, K^{alg} une clôture algébrique de K contenant E. Soient σ un élément de $\mathrm{Hom}_K(E, K^{\mathrm{alg}})$ et σ' un prolongement de σ à K^{alg}. Alors l'ensemble des prolongements de σ à L est*

$$\{\sigma' \circ \tau \ / \ \tau \in \mathrm{Hom}_E(L, K^{\mathrm{alg}})\}.$$

En effet, pour τ décrivant $\mathrm{Hom}_E(L, K^{\mathrm{alg}})$, les $\sigma' \circ \tau$ sont des prolongements de σ et sont au nombre de $[L : E] = \mathrm{card}(\mathrm{Hom}_E(L, K^{\mathrm{alg}}))$, on les a donc tous.

Finissons la preuve du théorème. On reprend les notations utilisées auparavant. On pose de plus $H_{L/E} = \mathrm{Hom}_E(L, K^{\mathrm{alg}})$ et pour tout $\sigma_i \in H_{E/K}$ soit σ'_i l'un de ses prolongements à K^{alg}. Soit $x \in L$, le lemme montre que l'on a dans K^{alg}

$$\mathrm{N}_{L/K}(x) = \prod_{1 \leq i \leq d, \tau \in H_{L/E}} \sigma'_i \circ \tau(x),$$

par suite

$$\mathrm{N}_{L/K}(x) = \prod_{1 \leq i \leq d} \sigma'_i\Big(\prod_{\tau \in H_{L/E}} \tau(x)\Big) = \prod_{1 \leq i \leq d} \sigma'_i(\mathrm{N}_{L/E}(x)),$$

d'où, puisque σ_i et σ'_i coïncident sur E,

$$\mathrm{N}_{L/K}(x) = \prod_{1 \leq i \leq d} \sigma_i(\mathrm{N}_{L/E}(x)) = \mathrm{N}_{E/K}(\mathrm{N}_{L/E}(x)).$$

La formule pour la trace se montre de même. □

Remarque 3.7.4. les notations et hypothèses sont celles du lemme 3.7.3. On a aussi que l'ensemble des prolongements de σ à L est

$$\{\tau \circ \sigma' \ / \ \tau \in \mathrm{Hom}_E(L, K^{\mathrm{alg}})\}.$$

Le théorème suivant donne une propriété majeure de la trace.

Théorème 3.7.5. *Soit L/K une extension séparable finie. Alors l'application*

$$\begin{array}{rccc} \mathrm{Tr}: & L \times L & \to & K \\ & (x, y) & \mapsto & \mathrm{Tr}(xy) \end{array}$$

est une forme bilinéaire symétrique non dégénérée.

Démonstration. Il faut montrer qu'étant donné un élément x de L, si

$$(*) \quad \text{pour tout } y \in L, \quad \mathrm{Tr}_{L/K}(xy) = 0,$$

alors $y = 0$. Soit K^{alg} une clôture algébrique de K et posons

$$\mathrm{Hom}_K(L, K^{\mathrm{alg}}) = \{\sigma_1, \cdots, \sigma_d\}.$$

Désignons par $\mathcal{L}(L^*, K^{\mathrm{alg}})$ l'ensemble des applications de L^* dans K^{alg}, c'est un K^{alg}-espace vectoriel et l'on a

$$\mathrm{Hom}_K(L, K^{\mathrm{alg}}) \subset \mathcal{L}(L^*, K^{\mathrm{alg}}).$$

La relation $(*)$ s'écrit dans $\mathcal{L}(L^*, K^{\mathrm{alg}})$

$$\sum_{1 \leq i \leq d} \sigma_i(x)\sigma_i = 0,$$

le lemme suivant (appliqué à $L^* = G$ et $K^{\mathrm{alg}} = E$) montre qu'il en résulte $\sigma_i(x) = 0$ pour tout i, donc $x = 0$. □

Lemme 3.7.6. *(Emil ARTIN) Soient G un groupe et E un corps. Soient $\chi_1, \ldots, \chi_r$ des caractères distincts de G, à valeurs dans E^* (c'est à dire des homomorphismes distincts de groupes, définis sur G et à valeurs dans E^*). Alors $\chi_1, \ldots, \chi_r$ sont linéairement indépendants, dans le E-espace vectoriel des applications de G dans E.*

Démonstration. Considérons une relation de dépendance linéaire

$$(*) \quad 0 = a_1\chi_{i_1} + \cdots + a_n\chi_{i_n}$$

dans l'ensemble des applications de G dans E, avec donc les a_i dans E, non tous nuls. Les hypothèses montrent qu'une telle relation possède au moins deux termes.

Supposons n minimal (donc, en particulier, les a_i sont tous non nuls). Comme $\chi_{i_1} \neq \chi_{i_2}$, il existe $g \in G$ tel que $\chi_{i_1}(g) \neq \chi_{i_2}(g)$. Il suit de $(*)$ que

$$0 = a_1\chi_{i_1}(gh) + \cdots + a_n\chi_{i_n}(gh)$$

$$= a_1\chi_{i_1}(g)\chi_{i_1}(h) + \cdots + a_n\chi_{i_n}(g)\chi_{i_n}(h)$$

pour tout $h \in G$, d'où, dans l'ensemble des applications de G dans E

$$0 = a_1\chi_{i_1}(g)\chi_{i_1} + \cdots + a_n\chi_{i_n}(g)\chi_{i_n}.$$

On soustrait cette dernière formule à $(*)$ multiplié par $\chi_{i_1}(g)$, il vient

$$0 = a_2(\chi_{i_2}(g) - \chi_{i_1}(g))\chi_{i_2} + \cdots + a_n(\chi_{i_n}(g) - \chi_{i_1}(g))\chi_{i_n},$$

qui est une relation de dépendance linéaire car $\chi_{i_1}(g) \neq \chi_{i_2}(g)$. Ceci contredit la minimalité de n. □

Soit L/K une extension séparable finie. Il suit du théorème 3.7.5 que L et son dual $L^\vee$, en tant que K-espace vectoriel, sont canoniquement isomorphes : l'application

$$x \longmapsto (y \mapsto Tr_{L/K}(xy))$$

est un isomorphisme de L sur $L^\vee$. Si $\{e_1, \cdots, e_d\}$ est une base de L sur K, sa base duale via cet isomorphisme donne une base de L sur K, notée $\{e_1^\vee, \cdots, e_d^\vee\}$, elle est caractérisée par

$$\mathrm{Tr}_{L/K}(e_i e_j^\vee) = \delta_{i,j},$$

où $\delta_{i,j}$ est le symbole de Kronecker. Nous dirons que $\{e_1^\vee, \cdots, e_d^\vee\}$ *est la base duale de* $\{e_1, \cdots, e_d\}$ *relativement à la forme bilinéaire trace de* L *sur* K. La proposition suivante décrit une situation où la base duale est aisément calculable.

Proposition 3.7.7. *Soit* $L = K(x)$ *une extension séparable monogène du corps* K. *Soit* $P(X) = \mathrm{irr}(x, K; X)$, *posons* $d = [K(x) : K]$ *et écrivons dans* $K(x)[X]$

$$P(X) = (X - x)(a_0 + a_1 X + \cdots + a_{d-1} X^{d-1})$$

avec donc les a_i *dans* $K(x)$. *Alors, la base duale de* $\{e_i = x^{i-1}\}_{1 \le i \le d}$ *est*

$$\left\{ e_i^\vee = \frac{a_{i-1}}{P'(x)} \right\}_{1 \le i \le d}.$$

Démonstration. Soient K^{alg} une clôture algébrique de K, contenant x et $H = \mathrm{Hom}_K(K(x), K^{\mathrm{alg}})$. Il faut montrer que pour $0 \le i, j \le d-1$, on a

$$\mathrm{Tr}_{K(x)/K}(\frac{a_i}{P'(x)} x^j) = \delta_{i,j}.$$

Considérons

$$Q(X) = \sum_{0 \le i \le d-1} \mathrm{Tr}_{K(x)/K}(\frac{a_i}{P'(x)} x^j) X^i = \sum_{0 \le i \le d-1} \sum_{\sigma \in H} \sigma(\frac{a_i}{P'(x)} x^j) X^i,$$

on a

$$Q(X) = \sum_{\sigma \in H} (\sum_{0 \le i \le d-1} \sigma(a_i) X^i) \frac{\sigma(x)^j}{P'(\sigma(x))} = \sum_{\sigma \in H} \frac{P(X)}{X - \sigma(x)} \frac{\sigma(x)^j}{P'(\sigma(x))} = X^j$$

(on voit la dernière égalité en considérant la différence de ses deux membres, qui est un polynôme de degré au plus $d-1$ et qui s'annule en tous les $\sigma(x)$, $\sigma \in H$). Donc, pour $0 \le j \le d-1$

$$\sum_{0 \le i \le d-1} \mathrm{Tr}_{K(x)/K}(\frac{a_i}{P'(x)} x^j) X^i = X^j,$$

on en déduit les formules cherchées. □

Exercice 3.2. Une autre définition de la trace. Soient L/K une extension séparable finie et $x \in L$. Soit m_x l'application K-linéaire "multiplication par x", c'est à dire l'application de L dans lui-même, qui à $y \in L$ associe xy. Montrer que la trace de m_x est égale $\mathrm{Tr}_{L/K}(x)$, que le déterminant de m_x est égal à $\mathrm{N}_{L/K}(x)$ (on pourra d'abord supposer que $L = K(x)$ et utiliser la base $\{1, x, \cdots, x^{d-1}\}$ de L sur K, où $d = [K(x) : K]$, pour calculer les trace et déterminant de m_x).

3.8 Exercices

Séparabilité et Inséparabilité - Un petit résumé

Soient $K \subset M \subset L$ des extensions algébriques, et Ω un corps algébriquement clos contenant L.

1) **le degré de séparabilité de L sur K** $= [L : K]_s =$ le nombre des prolongements de $K \hookrightarrow \Omega$ à L. $[K(x) : K]_s =$ le nombre de racines distinctes du polynôme $\mathrm{irr}(x, K; X)$.

2) $[L : M]_s[M : K]_s = [L : K]_s$.

3) $x \in L$ est **séparable sur** K si $[K(x) : K]_s = [K(x) : K]$, i.e. les racines (ou la racine x) de $\mathrm{irr}(x, K) = P(X)$ sont simples (i.e. $P'(X) \neq 0$).

3') $x \in L$ est **purement inséparable sur** K si $[K(x) : K]_s = 1$, i.e. x est l'unique racine de $\mathrm{irr}(x, K; X)$.

4) L/K est **séparable** si tout élément de L est séparable sur K. Si L/K est finie, ceci est caractérisé par $[L : K]_s = [L : K]$ (en montrant que L/M et M/K sont séparables ssi L/K est séparable).

4') L/K est **purement inséparable** si tout élément de L est purement inséparable sur K. Ceci est caractérisé par $[L : K]_s = 1$ (Corollaire : L/M et M/K sont purement inséparables ssi L/K est purement inséparable).

5) Pour $S \subset L$, $K(S)/K$ est séparable ssi les éléments de S sont séparables sur K (soit $x \in K(S)$, se ramener au cas d'extension finie et utiliser 4)).

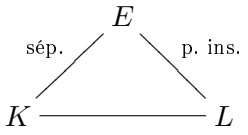
5') Pour $S \subset L$, $K(S)/K$ est purement inséparable ssi les éléments de S sont purement inséparables sur K.

6) Une extension finie séparable est monogène (Théorème de l'élément primitif).

Plus généralement, une extension finie est monogène ssi il n'y a qu'un nombre fini de sous-corps intermédiaires (**Théorème de l'élément primitif**). Le cas d'une extension finie séparable découle immédiatement du théorème fondamental de la théorie de Galois.

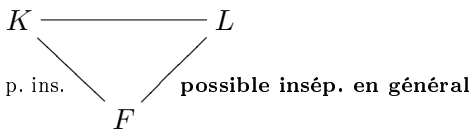
7) Soient $p =$ l'exposant caractéristique de K et $x \in L$, alors $\mathrm{irr}(x, K; X) = P(X) = Q(X^{p^\alpha})$ où $Q(X) \in K[X]$ est séparable, et $\alpha \in \mathbb{N}$, et l'on a $K(x^{p^\alpha})/K$ séparable et $K(x)/K(x^{p^\alpha})$ purement inséparable de degré $p^\alpha = \deg(P(X))/\deg(Q(X))$.

Ceci se généralise : soit $E = \{x \in L \mid x \text{ séparable sur } K\}$ (c'est un corps d'après 5)), on a

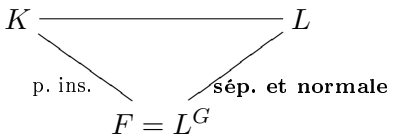


avec $[E : K] = [L : K]_s$ si L/K est finie. $[L : E] = \frac{[L:K]}{[L:K]_s} =$ une puissance de $p =$ **le degré d'inséparabilité de L sur K**.

7') Soit $F = \{x \in L \mid x \text{ purement inséparable sur } K\}$ (c'est un corps d'après 5')), on a



7") Si L/K est une extension **normale**, soit $G = \mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$, alors on a



Dans ce cas, on a L/L^G galoisienne, $[L : L^G] = [L : K]_s$ (si L/K finie), $L = EF$ et $E \cap F = K$.

8) En caractéristique $p > 0$, une extension finie purement inséparable est de degré une puissance de p (on se ramène aux extensions monogènes par 4'), et on applique 7)).

Exercice 3.3. Soit p un nombre premier. On considère le corps des fractions rationnelles $K = \mathbb{F}_p(T)$ et Ω une clôture algébrique de K.

1) Soit α une racine dans Ω de $f(X) = X^2 + TX + T$. Déterminer $[K(\alpha) : K]$ et montrer que $K(\alpha)/K$ est une extension normale. Est-elle séparable ?

2) Soit β une racine dans Ω de $h(X) = X^{2p} + TX^p + T$. Déterminer $[K(\beta) : K]$ et montrer que $K(\beta)/K(\alpha)$ est une extension purement inséparable. Déterminer $[K(\beta) : K]_s$.

3) Soit γ une racine de $g(X) = X^p + T$. Factoriser g puis h dans Ω.

Exercice 3.4. Soient K un corps séparablement clos, F une extension finie de K. Soit L une extension finie et séparable de F, montrer que $L = F$.

Exercice 3.5. Soient trois corps $K \subset F \subset L$ avec L/F normale et F/K purement inséparable. Montrer que L/K est normale. (**Remarque.** En particulier, toute extension purement inséparable est normale.)

Exercice 3.6. Soient K un corps de caractéristique $p > 0$ et $a \in K \setminus K^p$. Montrer que $X^p - a$ est irréductible sur K.

Exercice 3.7. Soient K un corps de caractéristique $p > 0$ et L une extension purement inséparable de K avec $[L : K] = p^n$. Montrer que $a^{p^n} \in K$ pour tout $a \in L$.

Exercice 3.8. (exemple d'une extension L/K telle que L n'est pas séparable sur la fermeture purement inséparable de K dans L) Soient k un corps de caractéristique 2, $K = k(x, y)$ le corps des fonctions rationnelles, $E = K(u)$ où u est une racine de $T^2 + T + x \in K[T]$ et $L = E(\sqrt{uy})$.

1) Montrer que L/E est purement inséparable et E/K est séparable. Montrer que $[L : E] = 2$ et $[E : K] = 2$.

2) Montrer que si $a \in L$ vérifie $a^2 \in K$, alors $a \in K$. En déduire que K est purement inséparablement clos dans L.

Exercice 3.9. Soit K le corps des fonctions rationnelles $k(x)$ sur un corps parfait k de caractéristique $p > 0$. Soient $u \in K, u \notin k$ et $E = k(u)$. Montrer que K/E est séparable si et seulement si $u \notin K^p$.

Exercice 3.10. Soient K une extension finie de F de caractéristique $p > 0$ avec $K^p \subset F$. Alors K/F est purement inséparable. Un ensemble $\{a_1, \ldots, a_n\} \subset K$ est dit une p-**base** de K/F s'il existe une suite d'extensions

$$F \subsetneqq F(a_1) \subsetneqq \cdots \subsetneqq F(a_1, \ldots, a_{n-1})(a_n) = K.$$

Montrer que si $\{a_1, \ldots, a_n\}$ est une p-base de K/F, alors $[K : F] = p^n$, en déduire que le nombre d'éléments dans une p-base est uniquement déterminé par K/F. Le nombre n est appelé la p-**dimension** de K/F. Montrer que K/F a une p-base.

Exercice 3.11. (exemple d'une extension finie ayant une infinité de sous-corps intermédiaire) Soient k un corps de caractéristique $p > 0$, $K = k(x, y)$ le corps des fonctions rationnelles sur k en deux variables et $F = k(x^p, y^p)$.

(a) Montrer que K/F est une extension purement inséparable de degré p^2.

(b) Montrer que $K \neq F(a)$ pour tout $a \in K$.

(c) Exhiber une infinité de sous-corps intermédiaires de l'extension K/F.

Exercice 3.12. Soient L/K une extension algébrique finie et $\mathcal{B} = \{a_1, \ldots, a_n\}$ une base du K-espace vectoriel L. Si $a \in L$, on définit $u_a : L \to L$ par $u_a(x) = ax$.

1) Montrer que u_a est K-linéaire. On note U_a sa matrice dans la base $\mathcal{B}$.

2) On suppose que L/K est séparable. On note $\{\sigma_i\}_{1 \leq i \leq n}$ les K-homomorphismes de L dans une clôture algébrique Ω et la matrice $A = (\sigma_i(a_j))_{1 \leq i,j \leq n}$.

i) Montrer que A est inversible.
ii) Montrer que U_a est semblable à la matrice diagonale $\mathrm{diag}(\sigma_1(a), \ldots, \sigma_n(a))$.
En déduire que $\mathrm{Tr}_{L/K}(a) = \mathrm{Tr}(u_a)$, et $\mathrm{N}_{L/K}(a) = \det(u_a)$.

Exercice 3.13. 1) Calculer $\mathrm{Tr}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\sqrt[3]{2})$ et $\mathrm{N}_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(\sqrt[3]{2})$.

2) Calculer $\mathrm{Tr}_{\mathbb{Q}(\sqrt[3]{2},j)/\mathbb{Q}}(\sqrt[3]{2})$ et $\mathrm{N}_{\mathbb{Q}(\sqrt[3]{2},j)/\mathbb{Q}}(\sqrt[3]{2})$.

3) Soient $[L : K] = n$ et $x \in L$. Soit $P(X) = X^d + a_1 X^{d-1} + \cdots + a_d$ le polynôme irréductible de x sur K. Montrer que $\mathrm{N}_{L/K}(x) = (-1)^n a_d^{\frac{n}{d}}$ et $\mathrm{Tr}_{L/K}(x) = -\frac{n}{d} a_1$.

Exercice 3.14. 1) Soit L/K une extension séparable finie. Montrer que $\mathrm{Tr}_{L/K}$ n'est pas une application nulle.

2) Soit K/F une extension de corps finis. Montrer que $\mathrm{N}_{K/F}$ est une application surjective.

Exercice 3.15. 1) Soient p un nombre premier impair, ξ une racine primitive p-ième de 1. Montrer que $\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(1 - \xi) = p$.

2) Soient $n \geq 3$, ζ une racine primitive n-ième de 1. Montrer que $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta) = 1$.

Chapitre 4

Théorie de Galois

Définition 4.0.1. Soit L/K une extension algébrique, on dit qu'elle est galoisienne si elle est normale et séparable.

Rappelons que le groupe de Galois d'une extension normale L sur K est $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ (groupe pour la composition des applications), que l'on a ensemblistement $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, \Omega)$ où Ω désigne n'importe quel corps algébriquement clos extension de L (cf. 2.2.1 et 2.2.4). Rappelons aussi que si H est un sous-groupe de $\mathrm{Gal}(L/K)$, on désigne par L^H le sous-corps des éléments de L invariants sous l'action de H, c'est à dire

$$L^H = \{x \in L \ / \ \sigma(x) = x \ \forall \sigma \in H\}.$$

Rappelons enfin qu'étant donné les propriétés des extensions séparables et des extensions normales, si L/K est une extension galoisienne finie, alors

$$[L : K] = o(\mathrm{Gal}(L/K)).$$

4.1 La correspondance de Galois

Théorème 4.1.1. *Soit L/K une extension galoisienne finie. Soient $\mathfrak{L}$ l'ensemble des corps intermédiaires entre K et L, $\mathfrak{G}$ l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$, soient*

- $\varphi : \mathfrak{L} \to \mathfrak{G}$ *l'application qui à $E \in \mathfrak{L}$ associe $\mathrm{Gal}(L/E)$,*
- $\psi : \mathfrak{G} \to \mathfrak{L}$ *l'application qui à $H \in \mathfrak{G}$ associe L^H.*

Alors φ et ψ sont des bijections décroissantes, réciproques l'une de l'autre.

De plus, soit E un élément de $\mathfrak{L}$, alors l'extension E/K est galoisienne si et seulement si $\mathrm{Gal}(L/E)$ est un sous-groupe normal de $\mathrm{Gal}(L/K)$; dans ce cas, la restriction des éléments de $\mathrm{Gal}(L/K)$ à E induit un isomorphisme canonique

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

Démonstration. Elle se déroule en plusieurs étapes.
1) On ne suppose pas ici que L/K est finie. Montrons que $\psi \circ \varphi = \mathrm{Id}_{\mathfrak{L}}$. Il faut prouver que pour tout $E \in \mathfrak{L}$ on a

$$E = L^{\mathrm{Gal}(L/E)}.$$

Posons $E' = L^{\mathrm{Gal}(L/E)}$. On a $E \subset E'$. Soit $x \in E'$ et supposons que $x \notin E$. Comme $\mathrm{irr}(x, E; X)$ a une racine dans L, il a une autre racine dans L (puisque $\deg(\mathrm{irr}(x, E; X)) > 1$ et que L est normal sur K, donc sur E) ; notons y cette deuxième racine. Soit $\sigma : E(x) \to L$ le morphisme trivial sur E et qui envoie x sur y, soient L^{alg} une clôture algébrique de L et $\tau : L \to l^{\mathrm{alg}}$ un prolongement de $E(x) \xrightarrow{\sigma} L \subset L^{\mathrm{alg}}$ à L. comme L est normal sur E, l'image de τ est dans L et τ est un élément de $\mathrm{Gal}(L/E)$, mais τ ne laisse pas fixe $x \in E' = L^{\mathrm{Gal}(L/E)}$. Ceci est une contradiction et montre que x n'existe pas.
2) On suppose de nouveau L/K finie. Montrons que $\varphi \circ \psi = \mathrm{Id}_{\mathfrak{G}}$. Il faut prouver que pour tout $H \in \mathfrak{G}$ on a

$$H = \mathrm{Gal}(L/L^H).$$

L'extension L/L^H est séparable et finie, donc il existe $x \in L$ tel que $L = L^H(x)$. Soit

$$P(X) = \prod_{\sigma \in H} (X - \sigma(x)).$$

C'est un élément de $L[X]$ et les fonctions symétriques des racines montrent que ses coefficients sont invariants sous l'action de H, donc $P(X) \in L^H[X]$. Il en résulte que $\mathrm{irr}(x, L^H, X)$ divise $P(X)$, puisque x est racine de $P(X)$. Donc $\deg(P) \geq [L : L^H]$, mais le degré de P est $o(H)$, par suite

$$o(H) \geq [L : L^H] = o(\mathrm{Gal}(L/L^H)),$$

De l'inclusion $H \subset \mathrm{Gal}(L/L^H)$ il vient l'inégalité inverse

$$o(\mathrm{Gal}(L/L^H)) \geq o(H).$$

On a prouvé $o(\mathrm{Gal}(L/L^H)) = o(H)$, donc $\mathrm{Gal}(L/L^H) = H$.
3) Soit H un sous-groupe normal de $\mathrm{Gal}(L/K)$, montrons que l'extension L^H/K est normale (il s'en suivra qu'elle est galoisienne). Soit $\sigma : L^H \to L^{\mathrm{alg}}$ un K-homomorphisme de L^H dans une clôture algébrique de L et soit τ un prolongement de σ à L, donc τ est dans $\mathrm{Gal}(L/K)$. Soit $\nu \in H$. On a $\tau' = \tau^{-1}\nu\tau$ qui est dans H, puisque ce dernier est normal dans $\mathrm{Gal}(L/K)$. Donc, pour tout $x \in L^H$, $\tau'(x) = x$, ce qui donne $\nu(\tau(x)) = \tau(x)$, ou encore $\nu(\sigma(x)) = \sigma(x)$. Donc, quel que soit le K-homomorphisme $\sigma : L^H \to L^{\mathrm{alg}}$ son image est dans L^H. Ceci prouve que L^H/K est normale.

Soit $E \in \mathfrak{L}$, supposons E/K galoisienne. Soit L^{alg} une clôture algébrique de L. Comme L/K et E/K sont normales, la restriction de L à E induit une application surjective

$$\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, L^{\mathrm{alg}}) \to \mathrm{Hom}_K(E, L^{\mathrm{alg}}) = \mathrm{Gal}(E/K),$$

son noyau est par $\mathrm{Gal}(L/E)$ d'après ce qui est prouvé en 2). Ainsi ce dernier est normal dans $\mathrm{Gal}(L/K)$ et l'on a l'isomorphisme cherché. □

Remarque 4.1.2. les notations sont celles du théorème. Cette correspondance, donnée par φ et ψ, entre $\mathfrak{L}$ et $\mathfrak{G}$, s'appelle la correspondance de Galois.

Remarque 4.1.3. On a vu que le point 1) de la démonstration ne nécessite pas que l'extension galoisienne L/K soit finie. Ce n'est pas du tout le cas au point 2). Lorsque L/K est infinie, la correspondance de Galois se fait avec les sous-groupes fermés de $\mathrm{Gal}(L/K)$, pour une certaine topologie, qui est la topologie triviale lorsque l'extension est finie. Le lecteur curieux pourra consulter par exemple le chapitre V du livre d'algèbre du traité de N. Bourbaki.

4.2 Compléments

Théorème 4.2.1. *Soient L/K et E/K deux extensions. On suppose que L/K est galoisienne finie. On suppose aussi que L et E sont des sous-corps d'un même troisième corps, de sorte que l'on peut définir leur compositum $L.E$. Alors $L.E$ est une extension galoisienne de E, l'application*

$$\mathrm{Gal}(L.E/E) \longrightarrow \mathrm{Gal}(L/K),$$

qui à $\sigma \in \mathrm{Gal}(L.E/E)$ associe sa restriction à L, est bien définie, elle induit un isomorphisme

$$\mathrm{Gal}(L.E/E) \simeq \mathrm{Gal}(L/L \cap E).$$

Démonstration. L'extension $L.E/E$ est séparable car $L.E = E(L)$ et L est séparable sur K, donc sur E.

Montrons que $L.E/E$ est normale. Soit un E-homomorphisme $\sigma : L.E \to \Omega$, où Ω est un corps algébriquement clos, extension de L et E. Alors la restriction $\sigma \mid L$ à L est un K-homomorphisme, donc $\sigma(L) = L$, puisque L/K est normale. Il vient $\sigma(L.E) = L.E$.

On a prouvé que l'extension $L.E/E$ est galoisienne, elle est aussi finie.

L'application

$$\varphi : \mathrm{Gal}(L.E/E) \longrightarrow \mathrm{Gal}(L/K),$$

qui à tout élément σ de $\mathrm{Gal}(L.E/E)$ associe sa restriction à L, est bien définie, car $\sigma \mid L$ est l'identité sur $L \cap E$, donc sur K et son image est L puisque L/K est normale ; de plus φ est injective : si l'on a $\sigma \mid L = \mathrm{Id}_L$, comme $\sigma \mid E = \mathrm{Id}_E$, il vient $\sigma \mid L.E = \mathrm{Id}_{L.E}$.

Montrons que l'image de φ est $\mathrm{Gal}(L/L \cap E)$. Puisque $L.E/E$ est galoisienne finie, suivant le théorème 4.1.1, il faut montrer que

$$L^{\mathrm{Im}\varphi} = E \cap L.$$

Soit $x \in L$ laissé stable par les éléments de $\mathrm{Im}\varphi$, comme φ est injectif, il suit que x, vu comme un élément de $L.E$, est laissé stable par tous les éléments de

$\mathrm{Gal}(L.E/E)$, donc (cf. 4.1.1) $x \in E$. On a prouvé $L^{\mathrm{Im}\varphi} \subset L \cap E$, l'inclusion inverse est évidente et a été remarquée plus haut. □

Le corollaire suivant est utile dans les applications concrètes.

Corollaire 4.2.2. *Soient L/K et E/K deux extensions. On suppose que L/K est galoisienne et finie. On suppose aussi que L et E sont des sous-corps d'un même troisième corps, de sorte que l'on peut définir leur compositum $L.E$. Alors*
(i) $[L.E : E]$ divise $[L : K]$, plus précisément

$$[L : K] = [L.E : E][L \cap E : K];$$

(ii) si $E \cap L = K$, on a

$$[L.E : E] = [L : K],$$

(iii) si $E \cap L = K$ et E/K est finie, on a de plus

$$[L.E : K] = [L : K][E : K].$$

Démonstration. Considérons le diagramme

$$\begin{array}{ccccc} & & E & & \\ & \nearrow & & \searrow & \\ K & & & & L.E \\ & \searrow & & \nearrow & \\ & & L & & \end{array}$$

où les flèches signifient des inclusions, on voit que le corollaire est une conséquence immédiate de l'isomorphisme de 4.2.1. □

Remarque 4.2.3. Le théorème 4.2.1 et son corollaire 4.2.2 sont faux sans l'hypothèse que l' extension L/K est galoisienne. Par exemple, soit

$$\begin{array}{ccccc} & & E = \mathbb{Q}(\sqrt[3]{2}) & & \\ & \nearrow & & \searrow & \\ K = \mathbb{Q} & & & & L.E = \mathbb{Q}(\sqrt[3]{2}, j) \\ & \searrow & & \nearrow & \\ & & L = \mathbb{Q}(j\sqrt[3]{2}) & & \end{array}$$

(j est une racine cubique de l'unité, $j \neq 1$). Les deux extensions L/K et E/K sont engendrées par des racines de $X^3 - 2$, elles sont donc de degré 3, comme E est inclus dans $\mathbb{R}$ on a $j \notin E$, donc $L.E/E$ est de degré 2 et 2 ne divise pas 3 (on a aussi $L.E/L$ de degré 2).

Exercice 4.1. Soit $\zeta \in \mathbb{C}$ une racine primitive 5-ième de l'unité, montrer que l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de degré 4. En déduire que $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})$ est aussi galoisienne de degré 4, que le degré de $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}$ est 12.

4.3 Le théorème de la base normale

L'objet de ce paragraphe est de montrer le

Théorème 4.3.1. *(Théorème de la base normale.) Soit L/K une extension galoisienne finie, alors il existe un élément x de L tel que L admette*

$$\{\sigma(x) \ / \ \sigma \in \mathrm{Gal}(L/K)\}$$

pour base sur K (une telle base est dite base normale de L sur K).

Nous donnons la démonstration d'abord lorsque K est infini.

Lemme 4.3.2. *Soient K un corps infini et L/K une extension galoisienne finie de degré n. Posons $\mathrm{Gal}(L/K) = \{\sigma_1, \cdots, \sigma_n\}$. Soit P un élément de $K[X_1, \cdots, X_n]$, non nul, alors il existe $x \in L$ tel que*

$$(*) \qquad P(\sigma_1(x), \cdots, \sigma_n(x)) \neq 0.$$

Démonstration. Soit P un élément de $K[X_1 \cdots, X_n]$ tel que, pour tout $x \in L$

$$P(\sigma_1(x), \cdots, \sigma_n(x)) = 0.$$

Soit $P = \sum_{0 \leq i \leq d} Q_i$ la décomposition de P en polynômes homogènes, Q_i étant de degré i. On a pour tout $\lambda \in K$

$$0 = P(\lambda\sigma_1(x), \cdots, \lambda\sigma_n(x)) = \sum_{0 \leq i \leq d} \lambda^i Q_i(\sigma_1(x), \cdots, \sigma_n(x)),$$

comme K est infini, il vient que pour tout $x \in L$ et tout $i = 0, \cdots, d$ on a $Q_i(\sigma_1(x), \cdots, \sigma_n(x)) = 0$. On peut donc supposer que P est homogène, de degré d minimal parmi les éléments de $K[X_1, \cdots, X_n]$ qui vérifient $(*)$.

Faisons donc ces hypothèses. Soit T une indéterminée, on a dans $K[T, X_1, \cdots, X_n]$

$$P(X_1 + T, \cdots, X_n + T) = \sum_{0 \leq i \leq d} R_i T^i,$$

où $R_i \in K[X_1 \cdots, X_n]$ est homogène de degré $d - i$. On en déduit que pour tous $x \in L$ et $\lambda \in K$

$$0 = P(\sigma_1(x) + \lambda, \cdots, \sigma_n(x) + \lambda) = \sum_{0 \leq i \leq d} \lambda^i R_i(\sigma_1(x), \cdots, \sigma_n(x)),$$

par suite, puisque K est infini et à cause de la minimalité de d, les polynômes $R_1, \cdots, R_d$ sont nuls. On a donc dans $K[T, X_1, \cdots, X_n]$

$$P(X_1 + T, \cdots, X_n + T) = P(X_1, \cdots, X_n),$$

en explicitant les deux polynômes de cette dernière formule, on voit que tous le coefficients de P sont nuls : P est le polynôme nul. □

Montrons le théorème, lorsque le corps K est infini. Posons $\mathrm{Gal}(L/K) = \{\mathrm{Id} = \sigma_1, \cdots, \sigma_n\}$ et soit dans l'anneau des polynômes $K[X_{\sigma_1}, \cdots, X_{\sigma_n}]$

$$P(X_{\sigma_1}, \cdots, X_{\sigma_n}) = \det\left(X_{\sigma_i^{-1}\sigma_j}\right)_{1\leq i,j\leq n},$$

ce n'est pas le polynôme nul car $P(1, 0, \cdots, 0)$ est le déterminant de la matrice identité, donc, d'après le lemme, il existe $x \in L$ tel que

$$P(\sigma_1(x), \cdots, \sigma_n(x)) \neq 0.$$

Montrons que $\{\sigma_1(x), \cdots, \sigma_n(x)\}$ est une base de L sur K. Sinon , il existe une relation du type

$$\sum_{1\leq j\leq n} a_j\sigma_j(x) = 0, \quad \text{avec} \quad a_j \in K,$$

d'où l'on déduit que pour tout $i = 1, \cdots, n$

$$\sum_{1\leq j\leq n} a_j\sigma_i^{-1}(\sigma_j(x)) = 0,$$

ce qui montre que

$$P(\sigma_1(x), \cdots, \sigma_n(x)) = \det\left(\sigma_i^{-1}(\sigma_j(x))\right)_{1\leq i,j\leq n} = 0,$$

ce qui est faux.

Démonstration du théorème, lorsque le corps K est fini. Nous verrons au chapitre 5, §2, que $\mathrm{Gal}(L/K)$ est alors cyclique, ce sont pour les extensions galoisiennes finies à groupes de Galois cycliques (qui sont appelées les extensions cycliques) que nous montrons maintenant le théorème. Posons $\mathrm{Gal}(L/K) =< \sigma >$ et $n = \circ(\mathrm{Gal}(L/K))$. On fait agir $K[X]$ sur L par

$$(1) \qquad \Big(P(X) = \sum_{0\leq i\leq d} a_iX^i, x\Big) \mapsto P(\sigma)(x) = \sum_{0\leq i\leq d} a_i\sigma^i(x),$$

où $P(X) = \sum_{0\leq i\leq d} a_iX^i$ et x désignent des éléments de $K[X]$ et L respectivement. Pour tout élément x de L soit

$$I(x) = \{P(X) \in K[X] \ / \ P(\sigma)(x) = 0\}.$$

On définit aussi

$$I = \{P(X) \in K[X] \ / \ \forall x \in L \ \ P(\sigma)(x) = 0\}.$$

Les $I(x)$ et I sont des idéaux de $K[X]$. Soit $\{x_1, \cdots, x_n\}$ une K-base de L, il est facile de vérifier que

$$(2) \qquad I = \bigcap_{1\leq j\leq n} I(x_j).$$

Construisons un élément x_0 de L tel que $I(x_0) = I$. Comme $K[X]$ est un anneau principal on écrit $I = (Q)$ et $I(x_j) = (Q_j)$ pour $1 \leq j \leq n$, où Q et les Q_j sont des éléments de $K[X]$. On pose aussi

$$Q = P_1^{m_1} \cdots P_r^{m_r},$$

où les P_i sont des éléments irréductibles de $K[X]$ (qui est un anneau factoriel), distincts à constantes multiplicatives près (c'est à dire que si $i \neq i'$, alors $P_i \neq \lambda P_{i'}$ pour tout $\lambda \in K^*$). La relation (2) montre que Q est un ppcm des (Q_j), $1 \leq j \leq n$, donc pour tout $i = 1, \cdots, r$, il existe j_i dans $\{1, \cdots, n\}$ tel que $P_i^{m_i}$ soit la plus grande puissance de P_i qui divise Q_{j_i}. Soit pour $1 \leq i \leq r$

$$Q^{(i)} = \prod_{1 \leq i' \leq r, i' \neq i} P_{i'}^{m_{i'}} \quad \text{et} \quad y_i = Q^{(i)} x_{j_i},$$

y_i est un élément de L et l'on a $I(y_i) = (P_i^{m_i})$. Soit $x_0 = y_1 + \cdots + y_r$, on a $I(x_0) = I$.

Montrons que $\{\sigma^0(x_0), \cdots, \sigma^{n-1}(x_0)\}$ est une K-base de L. Montrons d'abord que $I = (X^n - 1)$ (donc $Q(X) = X^n - 1$). On a $X^n - 1 \in I$, inversement, si $P(X) \in I$, on a (division euclidienne par $X^n - 1$ dans $K[X]$)

$$P(X) = (X^n - 1)P_1(X) + R(X),$$

avec $P_1(X)$ et $R(X)$ dans $K[X]$, $\deg R < n$. Le polynôme $R(X)$ est donc dans I, mais le lemme d'Artin 3.7.6 montre que $\mathrm{Id}, \sigma, \cdots, \sigma^{n-1}$, vus comme des applications de L^* dans lui-même, sont linéairement indépendants sur L, donc sur K, par suite $R(X) = 0$. On a donc prouvé que $I(x_0) = (X^n - 1)$, il en résulte que l'application $\varphi : K[X] \to L$, définie par $\varphi(P(X)) = P(\sigma)(x_0)$ induit un isomorphisme de K-espaces vectoriels

$$\frac{K[X]}{(X^n - 1)} \simeq \sum_{0 \leq i \leq n-1} K\sigma^i(x_0),$$

ceci prouve que $\sum_{0 \leq i \leq n-1} K\sigma^i(x_0)$ est de dimension n sur K, donc est égal à L. □

Remarque 4.3.3. La preuve du théorème de la base normale, lorsque le corps de base K est fini, pourrait être écrite avec le langage des modules introduit au chapitre 7 ; en effet, la relation (1) fait du groupe additif $(L, +)$ un $K[X]$-module de torsion.

4.4 Exercices

Une remarque

Soit L/K une extension finie contenu dans un corps algébriquement clos Ω, on a $|\mathrm{Gal}(L/K)| \leq |\mathrm{Hom}_K(L,\Omega)| = [L:K]_s \leq [L:K]$. 1er égalité ssi normale, 2e égalité ssi séparable. Ainsi deux égalités ssi galoisienne.

Exercice 4.2. Dans les questions suivantes, soient K un corps de décomposition de $P(X)$ sur F. Déterminer $\mathrm{Gal}(K/F)$ et trouver tous les sous-corps intermédiaires de K/F. Trouver un élément primitif de l'extension K/F.

(a) $F = \mathbb{Q}$ et $P(X) = X^3 - 2$.
(b) $F = \mathbb{Q}$ et $P(X) = X^4 - 7$.
(c) $F = \mathbb{F}_5$ et $P(X) = X^4 - 7$.
(d) $F = \mathbb{Q}$ et $P(X) = X^5 - 2$.
(e) $F = \mathbb{F}_2$ et $P(X) = X^6 + 1$.

Exercice 4.3. (a) Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Montrer que $K/\mathbb{Q}$ est une extension galoisienne. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Déterminer les sous-groupes de $\mathrm{Gal}(K/\mathbb{Q})$ et les corps d'invariants associés.

(b) Soient F un corps de caractéristique différente de 2, et K une extension galoisienne de F avec $[K:F] = 4$. Supposons que $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, montrer que $\exists a, b \in F$ tels que $K = F(\sqrt{a}, \sqrt{b})$.

Exercice 4.4. Soit L une extension galoisienne de K avec $[L:K] = n$. Si p est un diviseur premier de n, montrer qu'il existe un sous-corps E de L tel que $[L:E] = p$.

Exercice 4.5. Donner un exemple d'une extension K/F avec

(a) K/F normale et non galoisienne.
(b) K/F séparable et non galoisienne.

Exercice 4.6. Soit K une extension finie normale de F ($K \neq F$) telle qu'il n'y a pas de sous-extensions différentes de K et de F. Montrer que $[K:F]$ est premier. Donner un contre-exemple si K/F n'est pas normale.

Exercice 4.7. Soit $E \subset \mathbb{C}$ le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^7 - 8$.

(a) Déterminer E et calculer $[E:\mathbb{Q}]$.

(b) Soit $G = \mathrm{Gal}(E/\mathbb{Q})$. Montrer qu'il existe $\sigma \in G$ d'ordre 7 et $\tau \in G$ d'ordre 6 tels que $G = <\sigma, \tau>$.

Exercice 4.8. Soit $F \subset L \subset K$ avec L/F purement inséparable. Soit $a \in K$ séparable sur F. Montrer que $\mathrm{irr}(a, F) = \mathrm{irr}(a, L)$. Supposons maintenant K/L séparable et $[K : F] < \infty$. Soit S la clôture séparable de F dans K. Montrer que $K = SL$ et que $[K : L] = [S : F]$. (Remarque : L'exercice 3.4 est un cas particulier).

Exercice 4.9. Soient K/F une extension finie normale et L/F une extension finie algébrique. Si K/F ou L/F est séparable, montrer que $[KL : L] = [K : K \cap L]$.

Exercice 4.10. Soit $\mathbb{Q} \subset K \subset \mathbb{C}$ avec $K/\mathbb{Q}$ galoisienne. Soit σ la conjugaison complexe, montrer que $\sigma(K) = K$. Montrer que $K^{<\sigma>} = K \cap \mathbb{R}$ et que $[K : K \cap \mathbb{R}] \leq 2$. Donner deux exemples avec $[K : K \cap \mathbb{R}] = 1$ et $[K : K \cap \mathbb{R}] = 2$ respectivement.

Chapitre 5

Exemples d'extensions galoisiennes

5.1 Les extensions cyclotomiques

Définition 5.1.1. Soient K un corps et $n > 0$ un entier, on appelle racine n-ème de l'unité de K toute racine dans K du polynôme $X^n - 1$. On note $\mu_n(K)$ l'ensemble des racines n-ème de l'unité de K.

Proposition 5.1.2. *Soient K un corps et $n > 0$ un entier, posons $n = mp^\alpha$ où p est l'exposant caractéristique de K et m est premier avec p. On a*

$$\mu_n(K) = \mu_m(K),$$

soit $n' > 0$ un diviseur de n , alors

$$\mu_{n'}(K) \subset \mu_n(K),$$

$\mu_n(K)$ est un groupe cyclique d'ordre un diviseur de m, d'ordre m si K est algébriquement clos.

La seule chose à prouver est que $\mu_n(K)$ est cyclique, c'est une conséquence du lemme suivant.

Lemme 5.1.3. *Soient K un corps et G un sous-groupe fini du groupe multiplicatif K^*, alors G est cyclique.*

Démonstration. Posons $n = \circ(G)$. Pour tout diviseur d de n soit G_d l'ensemble des éléments de G d'ordre d. Evaluons le cardinal de G_d. Supposons que G_d soit non vide, soit x l'un de ses éléments, alors

$$< x >= \{1, x, x^2, \cdots, x^{d-1}\}$$

est un ensemble de d racines dans K, distinctes, du polynôme $X^d - 1$, c'est à dire que c'est l'ensemble de toutes les racines (dans K) de ce polynôme. Par

suite G_d est l'ensemble des générateurs du groupe cyclique $< x >$. Posons $\varepsilon_d = 1$ si $G_d \neq \emptyset$ et $\varepsilon_d = 0$ sinon, on a prouvé

$$\mathrm{card}(G_d) = \varepsilon_d \varphi(d),$$

où φ désigne l'indicateur d'Euler. Comme G est la réunion disjointe des G_d, pour d divisant n, il vient

$$(1) \qquad n = \sum_{d|n} \varepsilon_d \varphi(d).$$

Le même raisonnement, appliqué à un groupe cyclique connu, par exemple $(\mathbb{Z}/n\mathbb{Z}, +)$, donne (puisqu'alors, si d divise n, l'ensemble des éléments d'ordre d est non vide, de cardinal $\varphi(d)$)

$$(2) \qquad n = \sum_{d|n} \varphi(d).$$

La comparaison des formules (1) et (2) montre que l'on a toujours $\varepsilon_d = 1$, en particulier $\varepsilon_n = 1$. □

Définition 5.1.4. Soient K un corps et $n > 0$ un entier, un générateur de $\mu_n(K)$ s'appelle une racine primitive n-ème de l'unité de K.

Notons $\mathbb{Q}^{\mathrm{alg}}$ la clôture algébrique de $\mathbb{Q}$ contenue dans $\mathbb{C}$ et pour tout entier $n > 0$ posons $\Phi_n(X) = \prod(X - \zeta)$, où ζ décrit l'ensemble des racines primitives n-ème de l'unité de $\mathbb{Q}^{\mathrm{alg}}$.

Définition 5.1.5. Le polynôme $\Phi_n(X)$ s'appelle le n-ème polynôme cyclotomique.

Proposition 5.1.6. *Soit $n > 0$ un entier, alors*

$$\Phi_n(X) \in \mathbb{Z}[X].$$

Démonstration. Soit $G = \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$, l'action de G sur les racines de $\Phi_n(X)$ ainsi que les fonctions symétriques de ces mêmes racines montrent que $\Phi_n(X) \in (\mathbb{Q}^{\mathrm{alg}})^G[X]$, et il résulte de la première partie de la démonstration de 4.1.1 que $(\mathbb{Q}^{\mathrm{alg}})^G = \mathbb{Q}$. Ainsi $\Phi_n(X) \in \mathbb{Q}[X]$. La formule (évidente)

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

et 8.3.4 montrent alors que les polynômes cyclotomiques sont à coefficients entiers, puisqu'ils sont unitaires. □

Les polynômes cyclotomiques sont aussi irréductibles dans $\mathbb{Z}[X]$, cela résulte de l'étude suivante des extensions obtenues par adjonction de racines de l'unité.

Définition 5.1.7. Soient K un corps et $n > 0$ un entier. Lorsque K est de caractéristique non nulle on suppose que celle-ci ne divise pas n. Soient K^{alg} une clôture algébrique de K et ζ une racine primitive n-ème de l'unité dans K^{alg}. Le corps $K(\zeta)$ est appelé extension cyclotomique de K de niveau n.

Cette définition ne dépend pas du choix de la racine primitive, en fait on a avec les notations de la définition $K(\zeta) = K(\mu_n(K^{\mathrm{alg}}))$. Cette formule montre aussi que deux extensions cyclotomiques de K de même niveau sont K-isomorphes (cf. 2.1.3), mais la proposition suivante en dit plus.

Proposition 5.1.8. *Soient K un corps et $n > 0$ un entier, premier à la caractéristique de K lorsque celle-ci est non nulle. Soit $\alpha : \mathbb{Z} \to K$ l'application canonique, qui à l'entier z associe $z1_K$, où 1_K est l'élément unitaire de K ; notons $\Phi_n^\alpha(X) \in K[X]$ le polynôme obtenu par l'action de α sur les coefficients de $\Phi_n(X)$ (cf. 5.1.6). Soit E une extension cyclotomique de K de niveau n.*
(i) L'extension E/K est galoisienne. Soit $\zeta \in E$ une racine primitive de l'unité (donc $E = K(\zeta)$), alors $\mathrm{irr}(\zeta, K; X)$ *divise* $\Phi_n^\alpha(X)$.
(ii) Posons $G = \mathrm{Gal}(E/K)$ et soit $\zeta \in E$ une racine primitive de l'unité. Pour tout $\sigma \in G$ soit m_σ un entier tel que $\sigma(\zeta) = \zeta^{m_\sigma}$, alors l'application

$$\omega \ : \ G \longrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*,$$

qui à σ associe la classe de m_σ modulo n, est un morphisme injectif de groupes ; il suit que $[E : K]$ divise $\varphi(n)$.

Démonstration. (i) Soit $\zeta \in E$ une racine primitive de l'unité. On a $E = K(\zeta)$ et ζ est racine de $X^n - 1$, ce dernier étant séparable sur K, compte tenu de l'hypothèse faite sur n. Donc E/K est séparable. Cette extension est normale car E est un corps de décomposition de $X^n - 1$ sur K. Montrons que ζ est racine de $\Phi_n^\alpha(X)$: ζ est racine de

$$X^n - 1 = \prod_{d|n} \Phi_d^\alpha(X),$$

si ζ est racine de $\Phi_d^\alpha(X)$ pour $d < n$, puisque ce dernier divise $X^d - 1$ dans $K[X]$, il vient que ζ est racine de $X^d - 1$, ce qui est faux.

(ii) Soit $\sigma \in G$. Comme σ induit un isomorphisme de $\mu_n(E)$, $\sigma(\zeta)$ est aussi une racine primitive de l'unité, donc s'écrit $\sigma(\zeta) = \zeta^{m_\sigma}$ avec m_σ premier à n. Ceci montre que l'application ω est définie ; le fait qu'alors ce soit un morphisme injectif est facile. On a $[E : K]$ qui divise $\varphi(n)$ puisque $\omega(G)$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. □

Corollaire 5.1.9. *Soient $n > 0$ un entier et E une extension cyclotomique de $\mathbb{Q}$ de niveau n. Alors $[E : \mathbb{Q}] = \varphi(n)$, le polynôme cyclotomique $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$ (donc dans $\mathbb{Z}[X]$).*

Démonstration. Soient $G = \mathrm{Gal}(E/\mathbb{Q})$ et $\zeta \in E$ une racine primitive n-ème de l'unité. Il faut prouver que le morphisme

$$\omega \ : \ G \longrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

de 5.1.8 est surjectif, c'est à dire qu'il faut montrer que pour tout nombre premier l ne divisant pas n, il existe $\sigma \in G$ tel que $\sigma(\zeta) = \zeta^l$. Soient donc l un nombre premier ne divisant pas n, $P(X) = \mathrm{irr}(\zeta, \mathbb{Q}; X)$ et $Q(X) = \mathrm{irr}(\zeta^l, \mathbb{Q}; X)$. Il faut prouver que $P(X) = Q(X)$.

Supposons que $P(X) \neq Q(X)$. Les polynômes $P(X)$ et $Q(X)$ sont dans $\mathbb{Z}[X]$, car ils divisent $X^n - 1$ dans $\mathbb{Q}[X]$ et sont unitaires (cf. 8.3.4). Par le même argument, on peut écrire dans $\mathbb{Z}[X]$

$$X^n - 1 = P(X)Q(X)U(X) \quad \text{et} \quad Q(X^l) = P(X)V(X),$$

avec donc $U(X)$ et $V(X)$ dans $\mathbb{Z}[X]$. Nous allons examiner ces relations en réduisant les coefficients des polynômes modulo l, nous indiquons cette réduction en surlignant les polynômes. Il vient dans $(\mathbb{Z}/l\mathbb{Z})[X]$

$$X^n - \bar{1} = \bar{P}(X)\bar{Q}(X)\bar{U}(X) \quad \text{et} \quad (\bar{Q}(X))^l = \bar{P}(X)\bar{V}(X).$$

Soit $w(X)$ un élément irréductible de $(\mathbb{Z}/l\mathbb{Z})[X]$ divisant $\bar{P}(X)$, la deuxième relation montre que $w(X)$ divise $\bar{Q}(X)$ dans $(\mathbb{Z}/l\mathbb{Z})[X]$, la première relation montre alors que $w(X)^2$ divise $X^n - \bar{1}$ dans $(\mathbb{Z}/l\mathbb{Z})[X]$, mais ceci est impossible car $X^n - \bar{1}$ est séparable. □

Remarque 5.1.10. On reprend les notations et hypothèses de 5.1.8, il n'est pas fréquent que les polynômes $\Phi_n^\alpha(X)$ soient irréductibles dans $K[X]$, par exemple, on va voir au paragraphe suivant en 5.2.6, que si $K = \mathbb{F}_q$ est un corps fini à q éléments, si $n > 0$ est un entier non divisible par la caractéristique de $\mathbb{F}_q$, si E est une extension cyclotomique de $\mathbb{F}_q$ de niveau n, alors $[E : \mathbb{F}_q]$ est égal à l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.

5.2 Les corps finis

On note généralement $\mathbb{F}$ un corps fini, ou encore $\mathbb{F}_q$, pour rappeler son nombre q d'éléments. La caractéristique d'un corps fini est un nombre premier.

Proposition 5.2.1. *(i) Soit $\mathbb{F}$ un corps fini de caractéristique p, alors $\mathbb{F}$ est une extension finie de son sous-corps premier $\mathbb{F}_p$. Posons $n = [\mathbb{F} : \mathbb{F}_p]$, on a* $\mathrm{card}(\mathbb{F}) = p^n$.
(ii) Soit $L/\mathbb{F}_q$ une extension finie de degré n, où $\mathbb{F}_q$ est un corps à q éléments, alors $\mathrm{card}(L) = q^n$.

Démonstration. Le corps $\mathbb{F}$ est un espace vectoriel sur son sous-corps premier $\mathbb{F}_p$, de dimension finie puisqu'il est fini (lui-même forme un système générateur fini sur $\mathbb{F}_p$). On voit qu'il suffit de prouver (ii). Soit $\{e_1, \cdots, e_n\}$ une base de L sur $\mathbb{F}_q$, on a en tant qu'espaces vectoriels

$$L = \bigoplus_{1 \leq i \leq n} \mathbb{F}_q e_i,$$

dont il résulte la formule sur les cardinaux. □

On a vu que les corps finis sont parfaits (cf. 3.5.4), le théorème suivant dit que ce sont tous des corps de décompositions.

Théorème 5.2.2. *Soient p un nombre premier, $\mathbb{F}_p$ un corps à p éléments et $\mathbb{F}_p^{\mathrm{alg}}$ une clôture algébrique de $\mathbb{F}_p$. Alors pour tout entier $n > 0$ il existe un et un seul sous-corps de $\mathbb{F}_p^{\mathrm{alg}}$ à p^n éléments, c'est le corps de décomposition (dans $\mathbb{F}_p^{\mathrm{alg}}$) du polynôme $X^{p^n} - X$.*

Démonstration. Soit K un sous-corps de $\mathbb{F}_p^{\mathrm{alg}}$ à p^n éléments. Le groupe multiplicatif K^* a $p^n - 1$ éléments, donc tous ses éléments sont racines de $X^{p^n-1} - 1$, comme K possède p^n éléments, il suit que ses éléments sont les racines dans $\mathbb{F}_p^{\mathrm{alg}}$ du polynôme $X^{p^n} - X$. Ceci prouve l'unicité, l'existence provient du fait que les racines de $X^{p^n} - X$ dans $\mathbb{F}_p^{\mathrm{alg}}$ forment un corps (cela se vérifie par un calcul direct). □

Corollaire 5.2.3. *(i) Soient p un nombre premier et $n > 0$ un entier, alors deux corps à p^n éléments sont isomorphes.*
(ii) Soient p un nombre premier, $\mathbb{F}_p^{\mathrm{alg}}$ une clôture algébrique d'un corps $\mathbb{F}_p$ à p éléments, $n > 0$ et $m > 0$ deux entiers, $\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^m}$ les sous-corps de $\mathbb{F}_p^{\mathrm{alg}}$ à p^n et p^m éléments respectivement. Alors $\mathbb{F}_{p^n}$ est un sous-corps de $\mathbb{F}_{p^m}$ si et seulement si n divise m.

Démonstration. La partie (i) résulte du fait que les corps finis sont des corps de décomposition (cf. (ii) de 2.1.3). Montrons (ii). Supposons que n divise m et posons $m = nd$. On a $p^{nd} - 1 = (p^n - 1)h$ avec $h = 1 + p^n + \cdots + p^{n(d-1)}$, par suite les racines (dans $\mathbb{F}_p^{\mathrm{alg}}$) de $X^{p^n-1} - 1$ sont aussi racines de $X^{p^m-1} - 1$. Il suit que le sous- corps de $\mathbb{F}_p^{\mathrm{alg}}$ à p^n éléments est contenu dans celui à p^m éléments. Réciproquement, si $\mathbb{F}_{p^n}$ est un sous-corps de $\mathbb{F}_{p^m}$, on a alors $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$ qui divise $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$. □

Corollaire 5.2.4. *Soit $L/\mathbb{F}_q$ une extension algébrique d'un corps fini à q éléments. Alors elle est galoisienne. Si de plus $L/\mathbb{F}_q$ est finie, alors son groupe de Galois est cyclique, engendré par le $\mathbb{F}_q$-automorphisme qui à tout élément x de L associe x^q.*

Démonstration. Montrons que $L/\mathbb{F}_q$ est normale. Soit $P(X) \in \mathbb{F}_q[X]$, irréductible et ayant une racine x dans L, il faut montrer que $P(X)$ se décompose dans $L[X]$ en un produit de polynômes du premier degré (cf. 2.1.4 et 2.2.1). D'après le théorème 5.2.2, l'extension $\mathbb{F}_q(x)/\mathbb{F}_q$ est normale, donc comme $P(X)$ a une racine dans $\mathbb{F}_q(x)$, il se décompose en un produit de polynômes du premier degré dans $\mathbb{F}_q(x)[X]$, par suite dans $L[X]$.

Supposons $L/\mathbb{F}_q$ finie, de degré n et soit σ le $\mathbb{F}_q$-automorphisme défini dans l'énoncé. Montrons que $\circ(< \sigma >) = n$ (ceci équivaut à $< \sigma >= \mathrm{Gal}(L/\mathbb{F}_q)$). Soit $d \leq n$ tel que $\sigma^d = \mathrm{Id}_L$, alors pour tout x de L on a

$$x = \sigma^d(x) = x^{p^d},$$

donc tous les éléments de L sont racines du polynôme $X^{p^d} - X$. Ceci impose $d = n$. □

Définition 5.2.5. Les notations et hypothèses sont celles du corollaire 5.2.4. Soit σ le générateur du groupe de Galois $\mathrm{Gal}(L/\mathbb{F}_q)$, qui à x de L associe x^q, on dit que σ est un automorphisme de Frobenius de L. Si $q = p^n$, où p est la caractéristique de $\mathbb{F}_q$, on a $\sigma = \sigma_0^n$, où σ_0 est l' homomorphisme de Frobenius absolu de L (cf. 3.5.2).

Proposition 5.2.6. *Soient $\mathbb{F}_q$ un corps fini à q éléments, $n > 0$ un entier premier avec q et E une extension cyclotomique de $\mathbb{F}_q$ de niveau n. Alors $[E : \mathbb{F}_q]$ est égal à l'ordre de la classe de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.*

Démonstration. Soit $G = \mathrm{Gal}(E/\mathbb{F}_q$, considérons le morphisme injectif

$$\omega \ : \ G \longrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

de 5.1.8. Le groupe G est engendré par le morphisme de Frobenius σ, qui à tout x de $\mathbb{F}_q$ associe x^q, donc l'image de ω est un groupe cyclique engendré par $\omega(\sigma)$ qui est la classe de q modulo n. □

Nous terminons ce paragraphe en montrant le seul résultat de ce cours qui ne suppose pas à priori que les corps considérés sont commutatifs.

Théorème 5.2.7. *(Théorème de Wedderburn) . Les corps finis sont commutatifs.*

Démonstration. Soit K un corps fini (qui n'est donc pas supposé à priori commutatif), la méthode consiste à faire agir le groupe multiplicatif K^* sur lui même par conjugaison et à utiliser les informations dont on dispose sur les orbites, la formule des classes, etc. Soit $\mathbb{F}_q$ le centre de K, c'est à dire

$$(1) \quad \mathbb{F}_q = \{x \in K \ / \ xy = yx \ \forall y \in K\}$$

(la notation $\mathbb{F}_q$ signifie qu'il s'agit d'un corps à q éléments) ; étant donné $x \in K^*$, on désigne par $\mathrm{Orb}(x)$ et $\mathrm{Stab}(x)$ l'orbite de x et son stabilisateur dans K^* ; soit

$$(2) \quad K_x = \{y \in K \ / \ xy = yx\},$$

c'est un corps intermédiaire (non nécessairement commutatif) entre le centre $\mathbb{F}_q$ et K et l'on a

$$(3) \quad \mathrm{Stab}(x) = K_x^*;$$

on a aussi

$$(4) \quad \mathrm{Orb}(x) = \{yxy^{-1} \ / \ y \in K^*\}.$$

Désignons par n la dimension (en tant qu'espace vectoriel) sur $\mathbb{F}_q$ de K.

(5) Soient L un corps intermédiaire (non nécessairement commutatif) entre $\mathbb{F}_q$ et K, d sa dimension sur $\mathbb{F}_q$ (en tant qu'espace vectoriel), montrons que d divise n. Cela résulte de considérations semblables à celles de la démonstration de 5.2.1, à condition d'utiliser la notion d'espace vectoriel sur un corps non commutatif, ce que nous voulons éviter. On procède donc ainsi : les deux groupes multiplicatifs L^* et K^* ont pour ordres respectivement $q^d - 1$ et $q^n - 1$, par suite, puisque L^* est un sous-groupe de K^*, $q^d - 1$ divise $q^n - 1$, il suit que d divise n (en effet d est l'ordre de q dans $\mathbb{Z}/(q^d - 1)\mathbb{Z}$).

(6) Montrons que $q - 1$ est divisible par $\Phi_n(q)$, où Φ_n est le n-ème polynôme cyclotomique.

La formule des classes dit qu'il existe des éléments $x_1, \cdots, x_r$ de K^*, qui ne sont pas dans le centre $\mathbb{F}_q$ (c'est à dire dont les stabilisateurs sont distincts de K^*) tels que

$$(7) \quad \circ(K^*) = \circ(\mathbb{F}_q^*) + \sum_{1 \leq i \leq r} \frac{\circ(K^*)}{\circ(\mathrm{Stab}(x_i))}.$$

Désignons par d_i la dimension de K_{x_i} sur $\mathbb{F}_q$ (en tant qu'espace vectoriel), on a d_i qui divise n (cf. (5)), $d_i < n$ car $x \notin \mathbb{F}_q$ (cf. (1)) et il résulte des formules (3), (7) que

$$q^n - 1 = q - 1 + \sum_{1 \leq i \leq r} \frac{q^n - 1}{q^{d_i} - 1},$$

ce qui peut s'écrire

$$\prod_{d|n} \Phi_d(q) = q - 1 + \sum_{1 \leq i \leq r} \prod_{d|n, d \nmid d_i} \Phi_d(q),$$

qui montre que $\Phi_n(q)$ divise $q - 1$, puisque $d_i \neq n$ pour tout i.

On a

$$(8) \quad \Phi_n(q) = \prod (q - \zeta),$$

le produit étant étendu à toutes les racines primitives n-ème de l'unité dans $\mathbb{C}$. Il est facile de vérifier qu'étant donné une telle racine ζ, on a $\mid q-\zeta \mid > q-1$ si $n > 1$, il vient donc avec la formule (8)

$$\mid \Phi_n(q) \mid > (q-1)^{\varphi(n)} \quad \text{si} \quad n > 1,$$

où φ désigne l'indicateur d'Euler. Cette dernière formule avec (6) impliquent $n = 1$, donc $K = \mathbb{F}_q$. □

5.3 Sur les extensions cycliques

Définition 5.3.1. Soit L/K une extension galoisienne, on dit qu'elle est abélienne, resp. cyclique, si son groupe de Galois est abélien, resp. cyclique.

Nous avons déjà rencontré des extensions abéliennes, les extensions cyclotomiques. Il y a au moins une situation où cela donne beaucoup, puisque selon le théorème de Kronecker et Weber, les extensions cyclotomiques de $\mathbb{Q}$ contiennent toutes ses extensions abéliennes. Nous avons aussi rencontré des extensions cycliques, les extensions finies des corps finis (qui d'ailleurs sont cyclotomiques). Les résultats suivants permettent d'obtenir d'autres exemples d'extensions cycliques, nous ne faisons à cette occasion qu'effleurer des méthodes puissantes, pouvant conduire à des résultats beaucoup plus vastes[1].

Lemme 5.3.2. *(Théorème 90 de Hilbert.) Soient L/K une extension cyclique de degré n, $G = \mathrm{Gal}(L/K)$, σ un générateur de G et x un élément de L.*
(i) (Forme multiplicative.) On a $\mathrm{N}_{L/K}(x) = 1$ si et seulement s'il existe $y \in L$ tel que $x = y/\sigma(y)$.
(ii) (Forme additive.) On a $\mathrm{Tr}_{L/K}(x) = 0$ si et seulement s'il existe $y \in L$ tel que $x = y - \sigma(y)$.

Démonstration. (i) Supposons que $\mathrm{N}_{L/K}(x) = 1$ et, suivant E. Artin , posons

$$\tau = \mathrm{Id}_L + x\sigma + (x\sigma(x))\sigma^2 + \cdots + (x\sigma(x)\cdots\sigma^{n-2}(x))\sigma^{n-1};$$

c'est une application de L dans lui même, qui, d'après le Lemme d'Artin 3.7.6 , n'est pas l'application nulle. Soit $z \in L$ tel que $\tau(z) \neq 0$, alors on vérifie aisément que, sous l'hypothèse $\mathrm{N}_{L/K}(x) = 1$, on a $x = \tau(z)/\sigma(\tau(z))$. La réciproque est évidente.

(ii) On sait que la forme bilinéaire symétrique

$$\begin{array}{rccc} \mathrm{Tr}: & L \times L & \to & K \\ & (y,z) & \mapsto & \mathrm{Tr}(yz) \end{array}$$

[1] On pourra par exemple consulter le "Livre d'algèbre" de N. Bourbaki, ch. V "Corps commutatifs", §8 et 9 (éd. Masson), ainsi que le ch. X, §3, de l'ouvrage "Corps locaux" de J.P. Serre (éd. Hermann).

est non dégénérée (3.7.5), donc il existe $z \in L$ tel que $\mathrm{Tr}_{L/K}(z) = \mathrm{Tr}(1 \cdot z) \neq O$. Soit $y \in L$ ainsi défini :

$$y = \Big(\mathrm{Tr}_{L/K}(z)\Big)^{-1}\Big(x\sigma(z)+(x+\sigma(x))\sigma^2(z)+\cdots(x+\sigma(x)+\cdots+\sigma^{n-2}(x))\sigma^{n-1}(z)\Big).$$

Sous l'hypothèse $\mathrm{Tr}_{L/K}(x) = 0$, on voit que $x = y - \sigma(y)$. La réciproque est immédiate. □

Théorème 5.3.3. *(Extensions kummeriennes.) Soient K un corps et $n > 0$ un entier, on suppose que n est premier à la caractéristique de K, lorsque celle-ci est non nulle, et que K contient une racine primitive n-ème de l'unité.*
(i) Soit L une extension cyclique de K de degré n, alors il existe des éléments θ de L et a de K tels que $L = K(\theta)$ et $\mathrm{irr}(\theta, K; X) = X^n - a$.
(ii) Inversement, soit a un élément de K et soit L le corps obtenu en adjoignant une racine θ (racine prise dans une clôture algébrique de K) du polynôme $X^n - a \in K[X]$, alors L/K est une extension cyclique de degré un diviseur d de n et $\theta^d \in K$ (c'est à dire que $\mathrm{irr}(\theta, K; X) = X^d - \theta^d$).

Démonstration. (i) Soit $\zeta \in K$ une racine primitive n-ème de l'unité. On a $\mathrm{N}_{L/K}(\zeta^{-1}) = (\zeta^{-1})^n = 1$, donc (cf. (i) de 5.3.2) il existe $\theta \in L$ tel que $(\zeta^{-1}) = \theta/\sigma(\theta)$, où σ désigne un générateur de $\mathrm{Gal}(L/K)$. On a $\sigma(\theta) = \zeta\theta$, on voit que θ a n images distinctes par les éléments de $\mathrm{Gal}(L/K)$, puisque ζ est primitive, donc $L = K(\theta)$. D'autre part

$$\mathrm{irr}(\theta, K, X) = \prod_{0 \leq i \leq n-1} (X - \zeta^i\theta) = X^n - a$$

avec $a = \prod_{0 \leq i \leq n-1} \zeta^i\theta = \theta^n$.

(ii) Soient K^{alg} une clôture algébrique de K et $\theta \in K^{\mathrm{alg}}$ une racine de $X^n - a$. L'extension $K(\theta)/K$ est séparable car θ est racine de $X^n - a$ qui est un élément séparable de $K[X]$, elle est normale car $K(\theta)$ est un corps de décomposition de $X^n - a$ sur K, puisque ce dernier contient les racines n-èmes de l'unité. Donc $K(\theta)/K$ est galoisienne. Pour tout $\sigma \in \mathrm{Gal}(K(\theta)/K)$ posons $\sigma(\theta) = \eta_\sigma\theta$, où $\eta_\sigma \in \mu_n(K)$ est une racine n-ème de l'unité, alors l'application $\sigma \mapsto \eta_\sigma$ défini un morphisme injectif $\mathrm{Gal}(K(\theta)/K) \to \mu_n(K)$. Donc $\mathrm{Gal}(K(\theta)/K)$ est cyclique et son ordre d divise $\circ(\mu_n(K)) = n$. Finalement, on a

$$\mathrm{N}_{K(\theta)/K}(\theta) = \prod_{\sigma \in \mathrm{Gal}(K(\theta)/K)} (\eta_\sigma\theta) \quad \in K,$$

donc $\theta^d \in K$. □

Théorème 5.3.4. *(Les extensions d'Artin-Schreier.) Soit K un corps de caractéristique $p > 0$.*

(i) Soit L/K une extension cyclique de degré p, alors il existe $\theta \in L$ et $a \in K$ tels que $L = K(\theta)$ et que $\mathrm{irr}(\theta, K; X) = X^p - X + a$.
(ii) Inversement, soit $a \in K$, alors le polynôme $X^p - X + a$ de $K[X]$ est
- ou bien décomposé dans $K[X]$ en un produit de polynômes du premier degré,
- ou bien irréductible dans $K[X]$.

Supposons $X^p - X + a$ irréductible dans $K[X]$, alors, si θ en est une racine (dans une clôture algébrique de K), l'extension $K(\theta)/K$ est cyclique de degré p.

Démonstration. (i) On a $\mathrm{Tr}_{L/K}(-1) = -p = 0$, donc (cf. (ii) de 5.3.2) il existe $\theta \in L$ tel que $-1 = \theta - \sigma(\theta)$, où σ est un générateur de $\mathrm{Gal}(L/K)$. On voit que θ a n images distinctes par les éléments de $\mathrm{Gal}(L/K)$, donc $L = K(\theta)$. D'autre part, si $\mathbb{F}_p$ désigne le sous-corps premier de K, on a

$$\mathrm{irr}(\theta, K; X) = \prod_{0 \le i \le n-1} (X - \sigma^i(\theta)) = \prod_{\lambda \in \mathbb{F}_p} (X - \theta - \lambda)$$

$$= (X - \theta)^p - (X - \theta) = X^p - X + (-\theta^p + \theta),$$

donc $a = -\theta^p + \theta = -\mathrm{N}_{L/K}(\theta)$.

(ii) Soit, dans une clôture algébrique K^{alg} de K, une racine θ de $P(X) = X^p - X + a$. Les racines (dans K^{alg}) de ce polynôme sont les $\theta + \lambda$, où λ décrit le sous-corps premier $\mathbb{F}_p$ de K. Soit $L = K(\theta)$, on voit donc que L est une extension galoisienne de K. Soit d le degré de L sur K, on a $1 \le d \le p$. Il existe des éléments $\lambda_1, \cdots, \lambda_d$ de $\mathbb{F}_p$ tels que

$$\mathrm{Tr}_{L/K}(\theta) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\theta) = \sum_{1 \le i \le d} (\theta + \lambda_i),$$

on voit donc que $d\theta \in K$. Par suite, si $d < p$, θ est dans K, donc toutes les racines de $P(X)$ (dans K^{alg}) sont dans K. Si $d = p$, l'application qui à $\sigma \in \mathrm{Gal}(L/K)$ associe $\sigma(\theta) - \theta$ est un isomorphisme entre $\mathrm{Gal}(L/K)$ et $\mathbb{F}_p$, donc L/K est cyclique, de degré p. □

5.4 Une clôture algébrique de $\mathbb{R}$

Dans ce paragraphe nous montrons le

Théorème 5.4.1. *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Démonstration. Le corps $\mathbb{R}$ possède les deux propriétés suivantes :
(i) tout nombre réel positif possède un racine carré dans $\mathbb{R}$,
(ii) tout élément de $\mathbb{R}[X]$ de degré impair possède une racine dans $\mathbb{R}$.

Soit $i \in \mathbb{C}$ une racine carrée de -1, on sait que $\mathbb{C} = \mathbb{R}(i)$. Montrons que $\mathbb{R}(i)$ est algébriquement clos.

Soit M une extension algébrique de $\mathbb{R}(i)$ et soit L une extension galoisienne de $\mathbb{R}$ admettant M comme sous-corps (par exemple L est une fermeture normale de M sur $\mathbb{R}$). Montrons que $L = \mathbb{R}(i)$.

Soit $G = \mathrm{Gal}(L/\mathbb{R})$ et soit H un 2-sous-groupe de Sylow de G (2 divise l'ordre de G car $\mathbb{R}(i)/\mathbb{R}$ est une sous-extension de $L/\mathbb{R}$). Grâce au théorème de l'élément primitif on peut écrire $L^H = L(\alpha)$. Le polynôme $\mathrm{irr}(\alpha, \mathbb{R}, X)$ est un élément de $\mathbb{R}[X]$ de degré impair (ce degré est $\circ(G)/\circ(H)$), donc avec la propriété (ii) rappelée plus haut, il est de degré 1 : $L^H = \mathbb{R}$.

Ainsi G est un 2-groupe fini. Soit $G_1 = \mathrm{Gal}(L/\mathbb{R}(i)$. Supposons $G_1 \neq \{id\}$, alors G_1 possède un sous-groupe d'indice 2, que l'on note G_2 (cf. la remarque 5.4.2 suivante). L'extension $L^{G_2}/\mathbb{R}(i)$ est de degré 2, elle s'écrit

$$L^{G_2} = \mathbb{R}(i)(\beta),$$

où β est racine d'un polynôme de degré 2 à coefficients dans $\mathbb{R}(i)$. Mais un tel polynôme a toujours une racine dans $\mathbb{R}(i)$, comme le montre la remarque 5.4.3 plus bas. Il suit $G_1 = \{id\}$, donc $L = \mathbb{R}(i)$. □

Remarque 5.4.2. Soient p un nombre premier et H un p-groupe fini, $H \neq \{id\}$, alors H possède un sous-groupe d'indice p. C'est une conséquence de la propriété très forte selon laquelle le centre Z de H n'est pas trivial. Si $\circ(H) = p$, il est clair que H possède un sous-groupe d'indice p. Si $\circ(H) > p$, soit $s : H \to H/Z$ la surjection canonique, alors, par hypothèse de récurrence, H/Z possède un sous-groupe H_1 d'indice p et $s^{-1}(H_1)$ est un sous-groupe de H d'indice p.

Remarque 5.4.3. Tout élément de $\mathbb{R}(i)$ est un carré dans $\mathbb{R}(i)$ (donc en particulier le discriminant d'un polynôme du second degré). En effet soient a et b deux nombres réels et cherchons x et y tels que $(x + iy)^2 = a + ib$. Cette équation est équivalent aux deux relations $x^2 - y^2 = a$ et $xy = b/2$.On voit que x^2 et $-y^2$ sont racines de l'équation à coefficients réels

$$T^2 - aT - (b^2/4) = 0,$$

dont le discriminant est $\Delta = a^2 + b^2$, c'est un carré dans $\mathbb{R}$, par conséquent d'après la propriété (i) rappelée plus haut, cette équation admet deux racines réelles et l'on voit facilement que l'une est positive (c'est x^2), l'autre négative (c'est $-y^2$). Le cacul de x et y utilise encore (i).

5.5 Exercices

Exercice 5.1. Soit $\mathbb{F}_q$ un corps fini à q éléments. On note $J(d)$ le nombre des polynômes irréductibles et unitaires de degré d dans $\mathbb{F}_q[X]$. En décomposant $X^{q^n} - X$, montrer que

$$q^n = \sum_{d|n} d \cdot J(d).$$

Exercice 5.2. On note Φ_n le n-ième polynôme cyclotomique de $\mathbb{Q}^{ac} \subset \mathbb{C}$ ($n \geq 2$). Montrer que Φ_n est un polynôme réciproque (i.e. $\Phi_n(X) = X^{\deg(\Phi_n)}\Phi_n(1/X)$).

Exercice 5.3. Montrer que $\Phi_{2n}(X) = \Phi_n(-X)$ si n est impair ≥ 3, et $\Phi_{2n}(X) = \Phi_n(X^2)$ si n est pair.

Exercice 5.4. Montrer que si p premier ne divise pas n, alors $\Phi_{np}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}$.

Exercice 5.5. Soit $n = p_1^{a_1} \cdots p_r^{a_r}$ la factorisation de n en nombres premiers. Montrer que $\Phi_n(X) = \Phi_{p_1 \cdots p_r}(X^{p_1^{a_1-1} \cdots p_r^{a_r-1}})$.

Exercice 5.6. Montrer que pour tout nombre premier p, Φ_{12} est réductible dans $\mathbb{F}_p[X]$. En déduire que le polynôme $(X^2+1)(X^2+X+1)(X^2-3)$ a une racine dans $\mathbb{F}_p$.

Exercice 5.7. Soient F un corps fini et $n \geq 1$. Montrer qu'il existe un polynôme irréductible de degré n dans $F[X]$.

Exercice 5.8. Soient K/F une extension finie, séparable, de degré p premier, θ un élément primitif de l'extension et $P(X) = \mathrm{irr}(\theta, F; X) \in F[X]$. On note Ω une clôture algébrique de K et E le corps de décomposition de $P(X)$ sur F contenu dans Ω.

(a) Montrer que E/F est galoisienne et que $\mathrm{Gal}(E/F)$ contient un élément σ d'ordre p tel que $\{\theta, \sigma(\theta), \ldots, \sigma^{p-1}(\theta)\}$ soit l'ensemble des racines de $P(X)$.

(b) Montrer que si $P(X)$ a une racine $\alpha \neq \theta$ dans K, alors $K = E$ et $\mathrm{Gal}(K/F)$ est cyclique.

Exercice 5.9. Soit $K = \mathbb{Q}(\sqrt{a})$ avec $a \in \mathbb{Z}$ et $a < 0$. Montrer qu'il n'existe pas d'extension cyclique E de $\mathbb{Q}$ telle que $K \subset E$ et $4|[E : \mathbb{Q}]$.

Exercice 5.10. Soient F un corps de caractéristique $p > 0$ et $m \geq 2$ un entier.

1) On suppose que E/F est une extension cyclique de degré p^m. On note σ un générateur de $\mathrm{Gal}(E/F)$, $\tau = \sigma^{p^{m-1}}$ et $K = E^{<\tau>}$.

i) Montrer qu'il existe un $P(X) = X^p - X - \lambda \in K[X]$ et θ une racine de $P(X)$ telle que $E = K(\theta)$ et $\tau(\theta) = \theta + 1$.

ii) Montrer que $E = F(\theta)$ et $\sigma(\theta) = \theta + \beta$ où $\beta \in K$ est tel que $\mathrm{Tr}_{K/F}(\beta) = 1$ et $\sigma(\lambda) - \lambda = \beta^p - \beta$.

2) On suppose que K/F est une extension cyclique de degré p^{m-1} et on note σ un générateur de $\mathrm{Gal}(K/F)$. Soit $\beta \in K$ tel que $\mathrm{Tr}_{K/F}(\beta) = 1$.

i) Justifier l'existence de β.

ii) Montrer qu'il existe $\alpha \in K$ tel que $\sigma(\alpha) - \alpha = \beta^p - \beta$.

iii) Montrer que $f(X) = X^p - X - \alpha$ est irréductible dans $K[X]$.

iv) Soit θ une racine de $f(X)$ dans une clôture algébrique de K. Montrer que $K(\theta)/F$ est une extension cyclique de degré p^m dont le groupe de Galois est engendré par le prolongement σ' de σ défini par $\sigma'(\theta) = \theta + \beta$.

Chapitre 6

Les équations résolubles par radicaux

6.1 A propos des équations de degrés 2 à 5

6.1.1 Le degré 2

Soient K un corps de caractéristique différente de 2 et

$$P(X) = X^2 + aX + b \in K[X],$$

supposé irréductible. Il est facile de vérifier que $P(X)$ a deux racines dans le corps $K(\delta)$, où δ est un élément d'une clôture algébrique de K tel que $\delta^2 = a^2 - 4b$, c'est à dire tel que δ^2 soit le discriminant de $P(X)$. Les deux racines de $P(X)$ dans $K(\delta)$ s'écrivent

$$x_i = \frac{-a \pm \delta}{2} \quad , \quad i = 1, 2.$$

Lorsque K est de caractéristique 2, les racines de $P(X)$ (dans une clôture algébrique de K) engendrent une extension d'Artin-Schreier (cf. 5.3.4).

6.1.2 Le degré 3

Soient K un corps de caractéristique différente de 2 et 3 et

$$P(X) = X^3 + aX^2 + bX + c \in K[X].$$

En changeant X en $X - a/3$ (c'est à dire en remplaçant $P(X)$ par $\phi(P(X))$, où ϕ est le K-automorphisme de $K[X]$ qui envoie X sur $X - a/3$), on voit que l'on peut supposer que le polynôme s'écrit

$$P(X) = X^2 + bX + c \in K[X].$$

Dans une clôture algébrique K^{alg} de K, cherchons les racines de ce polynôme (c'est à dire les solutions de l'équation $P(X) = 0$). Soit x l'une de ces racines, posons $x = u + v$, la relation $P(x) = 0$ devient alors

$$(u^3 + v^3 + c) + (u + v)(3uv + b) = 0.$$

Cherchons alors u et v tels que

$$u^3 + v^3 + c = 0 \quad \text{et} \quad 3uv + b = 0.$$

De tels u et v vérifie

$$u^3 + v^3 = -c \quad \text{et} \quad u^3 v^3 = (\frac{-b}{3})^3,$$

c'est à dire que u^3 et v^3 sont solutions de l'équation du second degré à coefficients dans K

$$T^2 + cT + (\frac{-b}{3})^3 = 0$$

et l'on est ramené au paragraphe précédent. On obtient ainsi $x = u + v$ sous la forme d'une formule, appelée *formule de Cardan*[1], où figurent des "racines carrées et cubiques" (c'est le vocabulaire traditionnel lorsque $K = \mathbb{R}$).

Soit toujours le polynôme $P(X)$, que l'on suppose irréductible dans $K[X]$, mais on suppose seulement que la caractéristique de K n'est pas 3. Soit L l'extension de K engendrée par les racines de $P(X)$ dans K^{alg}, cherchons le degré $[L : K]$.

On sait que $[L : K] \geq 3$, on sait aussi que le groupe $\text{Gal}(L/K)$ s'injecte dans le groupe des permutations $\mathcal{S}_3$ (en envoyant un automorphisme sur la permutation des racines qu'il engendre), donc $[L : K]$ divise $3! = 6$. On a trouvé

$$[L : K] = 3 \text{ ou } 6.$$

Nous essayons maintenant de préciser les cas ou l'on a le degré 3, ou bien le degré 6. Notons x_1, x_2 et x_3 les racines de $P(X)$ (dans L) et soit

$$\delta = (x_1 - x_2)(x_2 - x_3)(x_1 - x_3),$$

C'est un élément de L et pour tout σ dans $\text{Gal}(L/K)$ on voit que $\sigma(\delta) = \pm\delta$, par suite, si

$$\Delta = \delta^2 = ((x_1 - x_2)(x_2 - x_3)(x_1 - x_3))^2,$$

alors Δ est invariant par les éléments de $\text{Gal}(L/K)$, donc est dans K (Δ s'appelle le *discriminant* de $P(X)$). On peut d'ailleurs vérifier, mais le calcul est un peu long, que si $P(X) = X^3 + bX + c$, alors $\Delta = -4b^3 - 27c^2$. On peut aussi vérifier (c'est un calcul facile) que *pour tout* $\sigma \in \text{Gal}(L/K)$, *on a* $\sigma(\delta) = \delta$ *si et seulement si* σ *donne une permutation paire des racines de*

[1] Gordano Cardan, savant italien, 1501-1576.

$P(X)$. Par conséquent, si $\delta \in K$, alors les éléments $\mathrm{Gal}(L/K)$ ne donnent pas les permutations impaires des racines, donc $[L : K] = 3$, au contraire, si $\delta \notin K$, alors $K(\delta)/K$ est une extension de degré 2, donc 2 divise $[L : K]$, par suite $[L : K] = 6$. On a montré :

Proposition 6.1.1. *Soient K un corps de caractéristique différente de 3, $P(X) \in K[X]$ un polynôme irréductible de degré 3 et L un corps de décomposition de $P(X)$ sur K. Alors $[L : K] = 3$ si et seulement si le discriminant de $P(X)$ est un carré dans K. Sinon $[L : K] = 6$.*

6.1.3 Le degré 4

La méthode suivante permet de ramener l'étude des équations de degré 4 à celles de degrés 2 et 3. Elle est due à Ferrari[2], un élève de Cardan.

Soient K un corps de caractéristique différente de 2 et 3 et $P(X) = X^4 + aX^3 + bx^2 + cX + d$ un élément de $K[X]$. Soit σ un élément de K. On a

$$X^4 + aX^3 = (X^2 + \frac{a}{2}X + \sigma)^2 - (2\sigma + \frac{a^2}{4})X^2 - a\sigma X - \sigma^2,$$

donc

$$P(X) = (X^2 + \frac{a}{2}X + \sigma)^2 - ((2\sigma + \frac{a^2}{4} - b)X^2 + (a\sigma - c)X + \sigma^2 - d).$$

Si $(2\sigma + \frac{a^2}{4} - b)X^2 + (a\sigma - c)X + \sigma^2 - d$ est un carré dans $K[X]$, c'est à dire s'il existe α et β dans K tels que

$$(2\sigma + \frac{a^2}{4} - b)X^2 + (a\sigma - c)X + \sigma^2 - d = (\alpha X + \beta)^2,$$

alors on a

$$P(X) = (X^2 + \frac{a}{2}X + \sigma - \alpha X - \beta)(X^2 + \frac{a}{2}X + \sigma + \alpha X + \beta)$$

et la recherche des racines se ramène à celle d'équations de degré 2.

Le polynôme $(2\sigma + \frac{a^2}{4} - b)X^2 + (a\sigma - c)X + \sigma^2 - d$ est un carré dans $K[X]$ si et seulement son discriminant est nul, c'est à dire si et seulement si

$$(a\sigma - c)^2 - 4(2\sigma + \frac{a^2}{4} - b)(\sigma^2 - d) = 0,$$

c'est une équation de degré 3 en σ.

[2]Ludovico Ferrari, mathématicien italien, 1522-1565.

6.1.4 Une équation de degré 5

Soit

$$P(X) = X^5 - 4X + 2 \in \mathbb{Q}[X],$$

c'est un élément irréductible de $\mathbb{Q}[X]$. Soit L le sous-corps de $\mathbb{C}$ qui est un corps de décomposition de $P(X)$ sur $\mathbb{Q}$ et posons $G = \mathrm{Gal}(L/K)$. Il est facile de constater, par exemple en étudiant les variations de la fonction réelle $x \mapsto P(x)$, que $P(X)$ admet dans $\mathbb{C}$ trois racines réelles, α_1, α_2 et α_3, deux autres racines qui ne sont pas réelles, α_4 et α_5. Soit τ la conjugaison complexe, on a donc

$$\tau(\alpha_i) = \alpha_i \ \text{ pour } \ i = 1, 2, 3 \ \text{ et } \ \tau(\alpha_4) = \alpha_5 \ , \ \tau(\alpha_5) = \alpha_4,$$

ainsi $\tau(L) = L$, c'est à dire que la conjugaison complexe restreinte à L, que l'on note encore τ, est un élément de G.

Considérons G comme un groupe opérant sur les racines de $P(X)$, c'est à dire comme un sous-groupe de $\mathfrak{S}_5$. Alors G contient une transposition, c'est la conjugaison complexe τ. D'autre part G contient un élément d'ordre 5 (car $5 = \deg(P)$ divise $[L : \mathbb{Q}] = \circ(G)$), qui est un cycle d'ordre 5 (on vérifie en effet aisément que les éléments de $\mathfrak{S}_5$ d'ordre 5 bougent nécessairement tous les α_i). Donc G contient un cycle d'ordre 5 et une transposition. Le lemme suivant montre alors que G est égal à $\mathfrak{S}_5$.

Lemme 6.1.2. *Soient $n \geq 2$ et $l \geq 1$ deux entiers, $\mathfrak{S}_n$ le groupe des permutations d'un ensemble $\{\alpha_i / i = 1, \cdots, n\}$ à n éléments, $c = (\alpha_1, \cdots, \alpha_n)$ un cycle d'ordre n et $\tau = (\alpha_{i_0}, \alpha_{j_0})$ une transposition, avec $l = \mid i_0 - j_0 \mid$. On suppose que l et n sont premiers entre eux, alors $\mathfrak{S}_n = < c, \tau >$.*

Démonstration. Tous les entiers sont écrits modulo n. On a

$$c^{-1}\tau c = (\alpha_{i_0 - 1}, \alpha_{j_0 - 1}),$$

donc $< c, \tau >$ contient toutes les transpositions (α_i, α_j) avec $l = \mid i - j \mid$.

Soient $\sigma = (\alpha_i, \alpha_j)$ une transposition, $m \geq 1$ un entier tel que $ml = j - i$ (modulo n, c'est ici qu'intervient l'hypothèse selon laquelle n et l sont premiers entre eux) et considérons les deux produits de transpositions

$$u = (\alpha_i, \alpha_{i+l})(\alpha_{i+l}, \alpha_{i+2l}) \cdots (\alpha_{i+(m-2)l}, \alpha_{i+(m-1)l})(\alpha_{i+(m-1)l}, \alpha_{i+ml}),$$

$$v = (\alpha_{i+(m-2)l}, \alpha_{i+(m-1)l})(\alpha_{i+(m-3)l}, \alpha_{i+(m-2)l}) \cdots (\alpha_{i+l}, \alpha_{i+2l})(\alpha_i, \alpha_{i+l}),$$

alors il n'est pas difficile de vérifier que $\sigma = uv$. Ainsi toutes les transpositions sont dans $< c, \tau >$, ce dernier est donc égal à $\mathfrak{S}_n$. □

6.1.5 Conclusion

On se restreint dans ces commentaires au cas où le corps de base est $\mathbb{Q}$. On vient de voir que les équations de degrés 2, 3 et 4 sont "résolubles par radicaux" (ce vocabulaire sera précisé plus loin), c'est à dire que l'on obtient un corps contenant leurs racines en adjoignant à $\mathbb{Q}$ une racine n_1-ème de l'un de ses éléments (n_1 est un entier positif), puis en adjoignant au corps ainsi obtenu une racine n_2-ème de l'un de ses éléments, etc. On fait ceci un nombre fini de fois. On va montrer plus loin que l'existence d'une telle construction est équivalente au fait suivant : si $L/\mathbb{Q}$ est l'extension engendrée par les racines de l'équation, alors le groupe de Galois $\mathrm{Gal}(L/K)$ est résoluble.

L'exemple de l'équation

$$X^5 - 4X + 2 = 0$$

montre que *dès le degré 5, il existe des équations sur $\mathbb{Q}$ qui ne sont pas résolubles par radicaux* ; le groupe de Galois du corps engendré sur $\mathbb{Q}$ par les racines de l'équation est ici isomorphe à $\mathcal{S}_5$, qui n'est pas résoluble ; c'est la conséquence de 6.2.4 rappelé plus bas et du résultat classique suivant.

Lemme 6.1.3. *Pour $n \geq 5$ le groupe alterné $\mathcal{A}_n$ est simple.*

Démonstration. On fait opérer le groupe $\mathcal{A}_n$ sur l'ensemble d'entiers $\{1, 2, \cdots, n\}$, $n \geq 5$. Soit H un sous-groupe normal de $\mathcal{A}_n$, $H \neq \{\mathrm{Id}\}$.

1) $\mathcal{A}_n$ est engendré par les cycles d'ordre 3. En effet $\mathcal{A}_n$ est engendré par les produits de deux permutations ; soient des entiers $0 \leq a < b < c < d \leq n$, on a

$$(a,b)(b,c) = (a,b,c) \quad \text{et}$$

$$(a,b)(c,d) = ((a,b)(b,c))((b,c)(c,d)) = (a,b,c)(b,c,d).$$

2) Supposons que H contienne un cycle d'ordre 3, alors $H = \mathcal{A}_n$. En effet, soient σ un élément de H et (a,b,c) un cycle d'ordre 3, on sait que

$$\sigma(a,b,c)\sigma^{-1} = (\sigma(a), \sigma(b), \sigma(c)),$$

donc si H contient un cycle d'ordre 3, il les contient tous.

Il reste donc à prouver que H contient un cycle d'ordre 3. Soit c un élément de H, $c \neq \mathrm{Id}$ et de support minimal. On écrit

$$(1) \quad c = c_1 c_2 \cdots c_r$$

où les c_i sont des cycles à supports disjoints ; on note d_i le cardinal du support de c_i.

3) On a $d_1 = d_2 = \cdots = d_r$, on notera d cet entier. En effet, supposons les c_i numérotés de telle manière que la suite des n_i soit croissante et soit i_0 tel que

$$d_1 = \cdots = d_{i_0} < d_{i_0+1} \leq \cdots \leq d_r,$$

alors on a, puisque les c_i commutent entre eux, leurs supports étant disjoints,

$$c^{d_1} = c_1^{d_1} \cdots c_{i_0}^{d_1} c_{i_0+1}^{d_1} \cdots c_r^{d_1} \quad \text{donc} \quad c^{d_1} = c_{i_0+1}^{d_1} \cdots c_r^{d_1} \neq \mathrm{Id}$$

et ceci contredit la minimalité du support de c.

4) *Le cas* $r = 1$ (cf. la formule (1)). On a $d \geq 3$, posons

$$c = (a_1, \cdots, a_d)$$

et soit $\alpha = (a_1, a_2, a_3)$. Posons $\mu = c^{-1}(\alpha c \alpha^{-1})$, c'est un élément de H et l'on vérifie que $\mu = (a_1, a_2, a_d)$ est un cycle d'ordre 3.

5) *Le cas* $r > 1$. Posons dans la formule (1)

$$c_1 = (a_1, \cdots, a_d) \quad \text{et} \quad c_2 = (b_1, \cdots, b_d),$$

soient $\beta = (a_1, a_2, b_1)$ et $\nu = c^{-1}(\beta c \beta^{-1})$, ce dernier est un élément de H et l'on a

$$\nu = c_1^{-1} c_2^{-1} \beta c_1 c_2 \beta^{-1}.$$

Supposons que $d = 2$, on vérifie alors que

$$\nu = (a_1, b_1)(a_2, b_2).$$

Comme $n \geq 5$ il existe $z \in \{1, 2, \cdots, n\}$ tel que $z \neq a_1, a_2, b_1, b_2$, soit $\gamma = (a_1, b_1, z)$, on vérifie que $\gamma = \mu\gamma\mu\gamma^{-1}$, par conséquent γ est dans H.

Supposons que $d > 2$. Alors on vérifie que ν est un cycle d'ordre 5 :

$$\nu = (a_1, b_1, a_2, b_d, a_d).$$

Soit $\delta = (a_1, b_1, a_2)$, alors on a

$$\nu^{-1}\delta\nu\delta^{-1} = (a_1, a_2, a_d) \in H.$$

□

La recherche de tels exemples d'équations à coefficients rationnels non résolubles par radicaux, ainsi que l'explication de ce phénomène, motivèrent les recherches d'Évariste Galois et le firent passer à la postérité. Dans le paragraphe suivant nous précisons cette notion d'équation résoluble par radicaux.

6.2 Les extensions résolubles

Définition 6.2.1. Soit L/K une extension finie, on dit qu'elle est résoluble si elle est séparable et si, étant donné une clôture algébrique L^{alg} de L, le groupe de Galois de la fermeture normale sur K de L dans L^{alg} est un groupe résoluble.

Remarque 6.2.2. On reprend les notations de la définition. Comme L/K est séparable et finie il existe $\alpha \in L$ tel que $l = K(\alpha)$, alors la fermeture normale N de L sur K dans L^{alg} est le corps engendré sur K par les racines dans L^{alg} de $\mathrm{irr}(\alpha, K; X)$. C'est une extension galoisienne de K, changer la clôture algébrique de L donne un tel corps qui lui est K-isomorphe, donc le fait que $\mathrm{Gal}(L/K)$ soit résoluble ne dépend pas du choix de L^{alg}.

Rappels. Nous rappelons ici brièvement la définition et quelques propriétés des groupes résolubles. Un groupe fini G (noté multiplicativement) est dit *résoluble* s'il possède une suite de sous-groupes

$$(*) \qquad G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

tels que G_i soit normal dans G_{i-1}, et que les quotients G_{i-1}/G_i soient abéliens, $1 \leq i \leq m$. Une telle suite de sous-groupes s'appelle une résolution de G. Il y a des théorèmes importants, dus à Schreier, Jordan et Hölder, qui montrent, qu'après raffinement, les résolutions d'un groupe sont essentiellement uniques. Nous n'en dirons rien, nous contentant d'énoncer les quelques propriétés dont nous avons besoin.

Lemme 6.2.3. *Soit G un groupe résoluble, alors G possède une résolution à quotients d'ordres premiers.*

Démonstration. On reprend les notations de $(*)$. Le groupe G_{i-1}/G_i est abélien et fini, il s'écrit

$$G_{i-1}/G_i = H_{i,1} \oplus \cdots \oplus H_{i,r_i}$$

où les $H_{i,j}$ sont les sous-groupes de Sylow de G_{i-1}/G_i. Soient

$$s_i : G_{i-1} \to G_{i-1}/G_i$$

la surjection canonique et pour tout $l = 0, \cdots, r_i - 1$

$$G_{i,l} = s_i^{-1}(\oplus_{1 \leq j \leq r_i - l} H_{i,j});$$

on pose aussi $G_{i,0} = G_i$. On voit alors que $G_{i,l+1}$ est un sous-groupe normal de $G_{i,l}$ et que les quotients

$$\frac{G_{i,l}}{G_{i,l+1}} \simeq H_{i,r_i - l}$$

$(0 \leq l \leq r_i)$, sont des p-groupes, pour différents nombres premiers p. En remplaçant dans $(*)$ $G_{i-1} \supset G_i$ par

$$G_{i-1} = G_{i,0} \supset G_{i,1} \supset \cdots \supset G_{i,r_i - 1} \supset G_{i,r_i} = G_i,$$

il vient une résolution de G dont les quotients sont de p-groupes, pour certains nombres premiers p. Soit donc, avec les notations de $(*)$, une résolution

de G telle que les groupes G_{i-1}/G_i soient des p-groupes, p premier. Un p-groupe fini non trivial possède un sous-groupe d'indice p (c'est d'autant plus facile à prouver ici que les p-groupes considérés sont abéliens), il en résulte qu'il possède une résolution dont les quotients sont d'ordre p. Ainsi G_{i-1}/G_i possède une résolution dont les quotients sont d'ordres premiers, notons cette résolution

$$\frac{G_{i-1}}{G_i} = \bar{H}_{i,0} \supset \bar{H}_{i,1} \supset \cdots \supset \bar{H}_{i,r_i}.$$

Soit $s_i : G_{i-1} \to G_{i-1}/G_i$ la surjection canonique, alors la résolution cherchée s'obtient en remplaçant dans $(*)$ $G_{i-1} \supset G_i$ par

$$G_{i-1} = s_i^{-1}(\bar{H}_{i,0}) \supset s_i^{-1}(\bar{H}_{i,1}) \supset \cdots \supset s_i^{-1}(\bar{H}_{i,r_i-1}) \supset s_i^{-1}(\bar{H}_{i,r_i}) = G_i,$$

en effet, les quotients de cette nouvelle résolution sont d'ordres premiers car pour tous i et l

$$\frac{s_i^{-1}(\bar{H}_{i,l})}{s_i^{-1}(\bar{H}_{i,l+1})} \simeq \frac{\bar{H}_{i,l}}{\bar{H}_{i,l+1}}.$$

□

Lemme 6.2.4. *Soient G un groupe fini et H un sous-groupe de G.*
(i) Si G est résoluble, alors il en est de même de H.
(ii) Si H est normal dans G, alors G est résoluble si et seulement si H et G/H le sont.

Démonstration. (i) Soit

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

une résolution de G, alors on a

$$H = H \cap G_0 \supseteq H \cap G_1 \supseteq \cdots \supseteq H \cap G_m = \{1\}$$

qui donne une résolution de H, les quotients sont bien abéliens puisque l'on a des injections canoniques

$$\frac{H \cap G_i}{H \cap G_{i+1}} \hookrightarrow \frac{G_i}{G_{i+1}},$$

$0 \leq i \leq m-1$.

(ii) Soit $s : G \to G/H$ la surjection canonique. Si G est résoluble, alors d'après (i) H l'est et (les notations sont celles de (i))

$$\frac{G}{H} = s(G_0) \supseteq s(G_1) \supseteq \cdots \supseteq s(G_m) = \{1\}$$

donne une résolution de G/H. En effet $s(G_{i+1})$ est normal dans $s(G_i)$ et les quotients $s(G_i)/s(G_{i+1})$ sont abéliens car l'on a

$$\frac{s(G_i)}{s(G_{i+1})} \simeq \frac{s^{-1}(s(G_i))}{s^{-1}(s(G_{i+1}))} = \frac{HG_i}{HG_{i+1}}$$

et la surjection

$$\frac{G_i}{G_{i+1}} \to \frac{G_i}{H \cap G_{i+1}} \simeq \frac{HG_i}{HG_{i+1}}.$$

Inversement, soient

$$H = H_0 \supset H_1 \supset \cdots \supset H_l = \{1\}$$

$$\frac{G}{H} = \bar{G}_0 \supset \bar{G}_1 \supset \cdots \supset \bar{G}_m = \{1\}$$

des résolutions de H et G/H. Soit $s : G \to G/H$ la surjection canonique, alors

$$G = s^{-1}(\bar{(}G_0) \supset s^{-1}(\bar{G}_1) \supset \cdots \supset s^{-1}(\bar{G}_m) = H = H_0 \supset H_1 \supset \cdots \supset H_l = \{1\}$$

est une résolution de G. □

Ces rappels donnent immédiatement le résultat suivant

Corollaire 6.2.5. *Une extension L/K est résoluble si et seulement si il existe une extension E/K galoisienne à groupe de Galois résoluble dont elle est une sous-extension.*

Démonstration. Soit une extension E/K galoisienne à groupe de Galois résoluble dont L/K est une sous-extension, soient N la fermeture normale sur K de L dans E, $G = \mathrm{Gal}(E/K)$ et $H = \mathrm{Gal}(N/K)$. Le lemme 6.2.4 montre que si G est résoluble, il en est de même de H. □

Définition 6.2.6. Soit L/K une extension finie, elle est dite résoluble par radicaux s'il existe une extension finie E/K, dont elle est sous-extension, possédant la propriété suivante : il existe une suite de corps intermédiaires

$$K = E_0 \subset E_1 \subset \cdots \subset E_m = E,$$

tels que les extensions E_{i+1}/E_i, $0 \leq i \leq m-1$, soient du type suivant

(1) $E_{i+1} = E_i(\alpha)$, où α est racine d'un polynôme de la forme $X^n - a \in E_i[X]$, l'exposant n étant premier à la caractéristique de K lorsque celle-ci est positive,

(2) E_{i+1}/E_i est une extension d'Artin-Schreier (cf. 5.3.4), c'est à dire $E_{i+1} = E_i(\alpha)$, où α est racine d'un polynôme de la forme $X^p - X + a \in E_i[X]$, $p > 0$ étant la caractéristique de K.

Définition 6.2.7. Soient K un corps et $P(X)$ un élément non constant de $K[X]$. On dit que l'équation

$$P(X) = 0$$

est résoluble par radicaux sur K si, étant donné une clôture algébrique K^{alg} de K, l'extension de K engendrée par les racines de $P(X)$ dans K^{alg} est résoluble par radicaux.

Le théorème suivant précise les exemples et commentaires du début de ce chapitre.

Théorème 6.2.8. *Soit L/K une extension. Elle est résoluble si et seulement si elle est résoluble par radicaux.*

Démonstration. Supposons que L/K est une extension résoluble. Soit E/K une extension galoisienne finie, à groupe de Galois $G = \mathrm{Gal}(E/K)$ résoluble et admettant L/K comme sous-extension (d'après 6.2.5 il n'est pas nécessaire de préciser plus E). Soient

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

une résolution de G *à quotients d'ordres premiers* (cf. 6.2.3) et $E_i = E^{G_i}$ le sous-corps de E des invariants sous l'action de G_i, $0 \leq i \leq m$. Soient $n = [E : K]$ et ζ une racine primitive n-ème de l'unité (dans une clôture algébrique de E). Considérons la suite d'extensions

$$(1) \quad K \subset K(\zeta) = E_0(\zeta) \subset E_1(\zeta) \subset \cdots E_m(\zeta) = E(\zeta),$$

ainsi que pour $1 \leq i \leq m$ les diagrammes

$$\begin{array}{ccccc} & & E_i & & \\ & \nearrow & & \searrow & \\ E_{i-1} & & & & E_i(\zeta) \\ & \searrow & & \nearrow & \\ & & E_{i-1}(\zeta) & & \end{array}$$

où les flèches signifie des inclusions ; il résulte de 4.2.1 un morphisme injectif de groupes

$$\mathrm{Gal}(E_i(\zeta)/E_{i-1}(\zeta)) \hookrightarrow \mathrm{Gal}(E_i/E_{i-1}),$$

donc les $\mathrm{Gal}(E_i(\zeta)/E_{i-1}(\zeta))$ sont d'ordres premiers, les théorèmes d'Artin-Schreier 5.3.4 ou de Kummer 5.3.3 montrent alors que (1) fait de L/K une extension résoluble par radicaux (il faut remarquer que l'adjonction aux E_i de ζ ne sert qu'à rendre possible l'application du théorème de Kummer).

Inversement, supposons l'extension L/K résoluble par radicaux. Soit

$$(2) \quad K = E_0 \subset E_1 \subset \cdots \subset E_m$$

où L est un sous-corps de E_m et où les extensions E_i/E_{i+1} sont du type de la définition 6.2.6. Soit $n = [E_m : K]$, quitte à adjoindre à E_m une racine primitive n-ème de l'unité et à remplacer (2) par

$$K \subset K(\zeta) = E_0(\zeta) \subset E_1(\zeta) \subset \cdots E_m(\zeta),$$

on peut supposer que

(3) toutes les extensions E_i/E_{i+1} de (2) sont de Kummer ou d'Artin-Schreier, en particulier elles sont galoisiennes.
Dans une clôture algébrique E_m^{alg} de E_m, soit N la fermeture normale de E_m. Montrons que l'extension N/K est résoluble.Posons

$$\text{Hom}_K(E_m, E_m^{\text{alg}}) = \{\sigma_1 = \text{Id}, \cdots, \sigma_d\},$$

on suppose $d > 2$, sinon il n'y a rien à démontrer. Pour $2 \leq i \leq d$ soit

$$E_{m,i} = E_m\sigma_2(E_m)\cdots\sigma_i(E_m)$$

(il s'agit de compositum de corps dans E_m^{alg}, remarquons que l'on a en particulier $E_{m,d} = N$) et considérons la suite d'extensions (pour $2 \leq i \leq d-1$)

$$(4_i) \quad E_{m,i} \subset E_{m,i}\sigma_{i+1}(E_1) \subset E_{m,i}\sigma_{i+1}(E_2)\cdots E_{m,i}\sigma_{i+1}(E_m) = E_{m,i+1}$$

(il s'agit encore de compositum dans E_m^{alg}). On a pour tout $j = 1, \cdots, m$

$$E_{m,i}\sigma_{i+1}(E_j) = (E_{m,i}\sigma_{i+1}(E_{j-1}))\Big(\sigma_{i+1}(E_j)\Big)$$

donc, d'après (3), les extensions

$$E_{m,i}\sigma_{i+1}(E_j)/E_{m,i}\sigma_{i+1}(E_{j-1})$$

sont galoisiennes, de plus il résulte de 4.2.1 et du diagramme

$$\begin{array}{ccccc} & & \sigma_{i+1}(E_j) & & \\ & \nearrow & & \searrow & \\ \sigma_{i+1}(E_{j-1}) & & & & E_{m,i}\sigma_{i+1}(E_j) \\ & \searrow & & \nearrow & \\ & & E_{m,i}\sigma_{i+1}(E_{j-1}) & & \end{array}$$

un morphisme injectif de groupes

$$\text{Gal}(E_{m,i}\sigma_{i+1}(E_j) \,/\, E_{m,i}\sigma_{i+1}(E_{j-1})) \hookrightarrow \text{Gal}(\sigma_{i+1}(E_j)/\sigma_{i+1}(E_{j-1})) \simeq \text{Gal}(E_j/E_{j-1}),$$

qui prouve que les extensions de (4_i) sont abéliennes. Le recollement des suites (4_i) d'extensions, suivant les i croissants, fournit une suite d'extensions de la forme

$$K = N_0 \subset N_1 \subset \cdots \subset N_r = N,$$

chacune des N_{j+1}/N_j étant une extension abélienne $(0 \leq j \leq r-1)$. Soit $G_j = \text{Gal}(N/N_j)$, la correspondance de Galois montre alors que

$$\text{Gal}(N/K) = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

est une résolution de $\text{Gal}(N/K)$. □

6.3 Exercices

Exercice 6.1. Soient K un corps, $P(X) \in K[X]$, et L un corps de décomposition de $P(X)$ sur K. Soit $G := \mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ que l'on appelle *groupe de Galois de $P(X)$ sur K* (Remarque : à un isomorphisme près, ce groupe est indépendant du choix de L).

1) Soit n le nombre de racines distinctes de $P(X)$. Montrer que G est isomorphe à un sous-groupe de S_n.

2) Si $P(X)$ est irréductible, montrer que G est isomorphe à un sous-groupe transitif de S_n (un sous-groupe H de S_n est dit *transitif* si $\forall i \neq j (1 \leq i, j \leq n)$, $\exists \sigma \in H$, tel que $\sigma(i) = j$).

3) Soit $P(X) \in \mathbb{Q}[X]$ irréductible de degré p premier. Supposons que $P(X)$ a exactement deux racines non réelles, montrer que son groupe de Galois est isomorphe à S_p.

Exercice 6.2. Soient K un corps, $P(X) \in K[X]$, et L un corps de décomposition de $P(X)$ sur K. On écrit $P(X) = (X - x_1)^{n_1} \cdots (X - x_r)^{n_r}$ avec $x_i \in L$ $(1 \leq i \leq r)$ et $x_i \neq x_j$ $(\forall i \neq j)$. Soient $Q(X) = (X - x_1) \cdots (X - x_r) = X^r + a_1 X^{r-1} + \cdots + a_r$ et $E = K(a_1, \ldots, a_r)$.

1) Montrer que L est un corps de décomposition de $Q(X)$ sur E.

2) Montrer que L/E est galoisienne.

3) Montrer que $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/E)$.

Exercice 6.3. Soient p un nombre premier, G un groupe fini et H un p-sous-groupe de G. On rappelle que $N(H) = \{g \in G | gHg^{-1} = H\}$ est le normalisateur de H dans G.

1) Montrer que $[N(H) : H] \equiv [G : H] \pmod{p}$. (Indication : On pourra faire opérer H sur $S = \{gH | g \in G\}$.)

2) Supposons $p | [G : H]$ (Par exemple G un p-groupe fini et H un sous-groupe propre de G). Montrer que $p \mid [N(H) : H]$. En déduire $N(H) \neq H$.

3) Soient G un groupe et $H < G$, on dit que H est un **sous-groupe maximal** de G si $H \neq G$ et $(H < K < G \Rightarrow K = H$ ou $K = G)$. Montrer que tout sous-groupe maximal d'un p-groupe fini est distingué et d'indice p.

Exercice 6.4. 1) Montrer que tout groupe abélien est résoluble.

2) Montrer que S_3 et S_4 sont résolubles.

3) Soit p un nombre premier, montrer que tout p-groupe fini est résoluble.

Exercice 6.5. Soient G un groupe et $G' = <aba^{-1}b^{-1} \mid a, b \in G>$ (G' s'appelle le **sous-groupe des commutateurs** ou **sous-groupe dérivé** de G, noté aussi $[G : G]$).

1) Montrer que $\forall f \in \mathrm{End}(G)$, on a $f(G') \subset G'$. En déduire que $G' \lhd G$.

2) Soit $N \lhd G$. Montrer que G/N est abélien si et seulement si $G' \subset N$.

3) Déduire de 2) que $\forall f \in \mathrm{Hom}(G, A)$ avec A abélien, il existe un unique $\overline{f} \in \mathrm{Hom}(G/G', A)$ tel que $\overline{f} \circ s = f$ où $s : G \to G/G'$ est l'homomorphisme canonique.

Exercice 6.6. Soit G un groupe. On note $G^{(1)} := G'$ le sous-groupe dérivé, $G^{(i)} := (G^{(i-1)})'$ pour tout $i \geq 2$. Montrer que $G^{(i)} \lhd G$ pour tout $i \geq 1$.

Exercice 6.7. Soit G un groupe. Montrer que G est résoluble si et seulement s'il existe $n \geq 1$ tel que $G^{(n)} = \{e\}$.

Exercice 6.8. Soient G, M deux groupes finis, $H < G$, et $f : G \to M$ un morphisme.

1) Montrer que $\forall k \geq 1$, $f(G^{(k)}) = (f(G))^{(k)}$.

2) Si G est résoluble, montrer que H et $f(G)$ sont résoluble.

3) Supposons $H \lhd G$. Montrer que si H et G/H sont résolubles, alors G est résoluble.

Exercice 6.9. Soit $n \geq 5$. Montrer que S_n n'est pas résoluble (Rappelons que A_n est un groupe simple).

Exercice 6.10. Soit G un groupe fini d'ordre ≥ 2.

1) Montrer que si G est résoluble, alors il existe $H \lhd G$ tel que H abélien et $H \neq \{e\}$.

2) Montrer que si G n'est pas résoluble, alors il existe $H \lhd G$ tel que $H' = H$ et $H \neq \{e\}$.

Exercice 6.11. Soient $H \lhd G$, $K < G$. Supposons que H et K sont résolubles, montrer que HK est résoluble.

Exercice 6.12. Soient p, q deux nombres premiers, $p \neq q$.

1) Montrer que tout groupe d'ordre pq est résoluble.

2) Montrer que tout groupe d'ordre p^2q est résoluble.

Remarque. Le cas général sera traité dans l'exercice 6.13.

Exercice 6.13. Soient p, q deux nombres premiers, $p \neq q$, et G un groupe d'ordre $p^n q$ ($n \in \mathbb{N}$). Nous allons montrer par récurrence sur n que G est résoluble (en même temps, on montre aussi que G n'est pas simple pour $n \geq 1$).

Le cas $n = 0$ est clair, on suppose $n \geq 1$. On pose l'hypothèse de récurrence : tout groupe d'ordre $p^k q$ est résoluble si $k \leq n - 1$.

1) On suppose que G contient un sous-groupe H distingué non trivial (i.e. G n'est pas simple). Montrer que G est résoluble.

2) On suppose G simple et on se propose d'obtenir une contradiction.

a) Montrer que G contient exactement q p-sous-groupes de Sylow.

b) On note D un sous-groupe de G qui est maximal dans l'ensemble des intersections de paires de p-sous-groupes de Sylow de G distincts, et soit $H = N_G(D)$, le normalisateur de D dans G. Montrer que

b-1) H a au moins deux p-sous-groupes de Sylow. (Indication : on pourra utiliser l'exercice 6.3 2))

b-2) H a exactement q p-sous-groupes de Sylow.

b-3) D est contenu dans tout p-sous-groupe de Sylow de G.

b-4) $D = \{e\}$.

c) Conclure.

Exercice 6.14. Soient K un corps, $f(X) \in K[X]$ irréductible de degré $n \geq 5$, et E un corps de décomposition de $f(X)$ sur K. Supposons que $\mathrm{Aut}_K(E) \cong S_n$. Soient $f(u) = 0, u \in E$.

a) Montrer que $K(u)/K$ n'est pas galoisienne, $[K(u) : K] = n$ et $\mathrm{Aut}_K(K(u)) = \{\mathrm{id}_{K(u)}\}$.

b) Montrer qu'il n'existe pas de $K \subset K(u) \subset L$ tel que L soit une extension résoluble par radicaux de K.

Exercice 6.15. Pour chaque $P(X)$ ci-dessous, dire si $P(X)$ est résoluble par radicaux sur $\mathbb{Q}$.

a) $P(X) = X^5 - 2$.

b) $P(X) = X^5 + 2X^3 - 8X + 2$.

c) $P(X) = X^6 - 6X^3 + 7$.

Exercice 6.16. Déterminer pour chaque $f(X) \in \mathbb{Q}[X]$ ci-dessous le groupe de Galois de $f(X)$ sur $\mathbb{Q}$, puis déterminer explicitement une chaine d'extensions prouvant la résolubilité par radicaux sur $\mathbb{Q}$ de l'équation $f(x) = 0$.

a) $f(X) = X^3 - 5X + 7$.

b) $f(X) = X^4 + 2X^3 - 2X^2 + 6X - 15$.

Exercice 6.17. Soient $\mathbb{F}_q$ un corps fini à $q = p^n$ éléments, avec p premier et n pair, et $K = \mathbb{F}_q(T)$. On note K^{ac} une clôture algébrique de K, θ une racine de $f(X) = X^{p^2} - TX + T$ et α une racine de $g(X) = X^{p^2-1} - T$ dans K^{ac}.

1) Montrer que $f(X)$ et $g(X)$ sont irréductibles dans $K[X]$.

2) Montrer que l'ensemble des racines de $f(X)$ est $\{\theta + u | u \cdot g(u) = 0\}$.

3) Montrer que $K(\alpha)/K$ est une extension galoisienne et déterminer $\mathrm{Gal}(K(\alpha)/K)$.

4) On note E le corps de décomposition de $f(X)$ dans K^{ac}. Montrer que $E = K(\alpha, \theta)$ et que E/K est une extension galoisienne de degré $p^2(p^2-1)$.

5) Montrer que $\mathrm{Gal}(E/K(\alpha))$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

6) Montrer que E/K est résoluble par radicaux.

Exercice 6.18. Soient $K = \mathbb{C}(T)$ et ξ une racine primitive n-ième de 1. On note σ le $\mathbb{C}$-automorphisme de K défini par $\sigma(T) = \xi T$ et par τ le $\mathbb{C}$-automorphisme de K défini par $\tau(T) = T^{-1}$.

1) Vérifier que $\sigma^n = \tau^2 = \sigma\tau\sigma\tau^{-1} = id_K$. En déduire que le sous-groupe $G =< \sigma, \tau >$ de $\mathrm{Aut}_{\mathbb{C}}(K)$ est de cardinal $2n$.

2) Soit $E = K^G$. Montrer que $E = \mathbb{C}(T^n + T^{-n})$ et justifier que K/E est une extension galoisienne de degré $2n$.

3) Donner des extensions intermédiaires justifiant que K/E est résoluble par radicaux.

Chapitre 7

A la recherche d'informations sur quelques groupes de Galois

L'objet de ce chapitre est le suivant. Soit P un élément irréductible de $\mathbb{Z}[X]$, on veut obtenir des informations sur le corps engendré sur $\mathbb{Q}$ par une racine de P, ses corps de décompositions..., à partir de propriétés des objets analogues attachés aux polynômes obtenus en réduisant les coefficients de P modulo des nombres premiers p, l'idée étant d'utiliser le caractère particulièrement simple des extensions de $\mathbb{F}_p$. Cette "réduction modulo p" de l'étude des extensions engendrées par P demande beaucoup d'outils algébriques pour être maîtrisée. Plus explicitement, soit $K/\mathbb{Q}$ une extension galoisienne finie ; on va construire un anneau A, qui sera le prolongement naturel de $\mathbb{Z}$ dans K et pour tout idéal maximal $p\mathbb{Z}$ de $\mathbb{Z}$ on montrera qu'il existe un idéal maximal $\mathfrak{P}$ de A, au dessus de $p\mathbb{Z}$, i.e. tel que $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ (cette dernière relation implique qu'il existe un morphisme canonique $\mathbb{Z}/p\mathbb{Z} \hookrightarrow A/\mathfrak{P}$) ; enfin on cherchera à relier $\mathrm{Gal}(A/\mathfrak{P}, \mathbb{Z}/p\mathbb{Z})$ avec $\mathrm{Gal}(K, \mathbb{Q})$. On fera aussi de même avec $\mathbb{F}_q(T)$ et $\mathbb{F}_q[T]$ aux places de $\mathbb{Q}$ et $\mathbb{Z}$, où $\mathbb{F}_q$ désigne un corps fini.

Tous les anneaux sont supposés commutatifs et unitaires, sauf mention du contraire les morphismes sont supposés échanger les unités, y compris les morphismes inclusions, c'est à dire qu'un sous-anneau est supposé avoir la même unité que l'anneau.

7.1 Les modules

7.1.1 Généralités

Soit A un anneau. Un *A-module* $(M, +, \cdot)$ est la donnée d'un groupe abélien $(M, +)$ muni d'une opération externe $A \times M \to M$, $(a, x) \mapsto ax$, telle que, pour tous a et b dans A et pour tous x et y dans M

$$a(bx) = (ab)x \quad , \quad 1x = x$$

$$a(x+y) = ax + ay \quad , \quad (a+b)x = ax + bx.$$

Un *sous-A-module* N du A-module M est un sous-groupe tel que, pour tous $a \in A$ et $x \in N$, $ax \in N$.

Exemple. les sous-A-modules du A-module A sont les idéaux de l'anneau A.

Un *homomorphisme* ou *morphisme* $f : M \to N$ de A-modules est une application du A-module M vers le A-module N telle que, pour tous $a \in A$ et $x, y \in M$

$$f(x+y) = f(x) + f(y) \quad , \quad f(ax) = af(x).$$

Soit $f : M \to N$ un morphisme de A-modules et soit M' (resp. N') un sous-module de M (resp. N). On vérifie sans peine que $f(M')$ (resp. $f^{-1}(N')$) est un sous-module de N (resp. M). En particulier $\mathrm{Ker}(f)$ est un sous-A-module de M et f est injectif si et seulement si $\mathrm{Ker}(f) = \{0\}$.

On a les notions évidentes de produits de modules, de sommes et sommes directes de sous-modules... Un A-module M est dit de *type fini* s'il existe une partie finie F de M telle que tout élément de M se mette sous la forme $\sum_{x \in F} a_x x$, avec $a_x \in A$. On écrit alors : $M = \sum_{x \in F} Ax$.

Les axiomes des A-modules sont formellement les mêmes que ceux d'espaces vectoriels, mais le fait que les scalaires ne décrivent pas un corps donne aux modules une nature très différente. Par exemple, $\mathbb{Q}$ est un $\mathbb{Z}$-module (pour $\mathbb{Z} \subset \mathbb{Q}$) et $\mathbb{Q}$ ne possède pas de base sur $\mathbb{Z}$; en effet, deux éléments de $\mathbb{Q}$ sont toujours liés sur $\mathbb{Z}$.

Soit M un A-module et soit M_{tors} le sous-A-module engendré par l'ensemble des éléments de M qui sont de torsion, c'est-à-dire des x de M pour lesquels il existe $a \in A$ tel que $a \neq 0$ et $ax = 0$ (donc M_{tors} est l'ensemble des sommes $\sum a_x x$, où a_x est dans A et où x décrit un ensemble fini d'éléments de torsion de M) ; M_{tors} est appelé *sous-module de torsion*. Par exemple, $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module égal à son sous-module de torsion, on dit que c'est un $\mathbb{Z}$-module de torsion.

7.1.2 Quotients

Soient M un A-module et N un sous-module de M. La relation sur M

$$\forall x, y \in M \quad x \mathcal{R} y \;\Leftrightarrow\; x - y \in N$$

est une relation d'équivalence compatible avec les opérations de M (toutes les relations d'équivalence compatible avec les opérations de M proviennent de cette manière d'un sous-module de M). L'ensemble quotient se note M/N, il est muni de la structure de A-module qui fait de la surjection canonique un morphisme.

Théorème 7.1.1. *Soient $f : M \to N$ et $g : M \to P$ deux morphismes de A-modules. On suppose g* ***surjectif****. Alors les assertions suivantes sont équivalentes :*
(i) il existe un morphisme $h : P \to N$ de A-modules, unique, tel que $h \circ g = f$,
(ii) $\mathrm{Ker}(g) \subseteq \mathrm{Ker}(f)$.

De plus, si (i) ou (ii) est vraie, on a
(iii) h est surjectif si et seulement f l'est,
(iv) h est injectif si et seulement si $\mathrm{Ker}(g) = \mathrm{Ker}(f)$.

La démonstration est la même que pour les groupes ou les anneaux.

7.1.3 Modules noethériens

Théorème 7.1.2. *Soit M un A-module. Les assertions suivantes sont équivalentes :*
(i) tout sous-A-module de M est de type fini,
(ii) toute suite croissante de sous-A-modules de M est stationnaire,
(iii) tout ensemble non vide de sous-modules de M possède un élément maximal (pour l'inclusion).

La démonstration est la même que pour les anneaux. Remarquons qu'un anneau est noethérien si et seulement si c'est un module noethérien sur lui-même.

Définition 7.1.3. Un A-module qui satisfait l'une de ces assertions du théorème 7.1.2 est dit noethérien.

Proposition 7.1.4. *Soit*

$$0 \to M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$$

une suite exacte (courte) de A-modules (i.e. u est un morphisme de A-modules injectif, v est un morphisme de A-modules surjectif, de plus $\mathrm{Im}(u) = \mathrm{Ker}(v)$*), alors M est un A-module noethérien si et seulement si M' et M'' le sont.*

Démonstration. Supposons M noethérien, alors on voit qu'il en est de même de M' et M'', avec par exemple l'assertion (i) de la définition.

Inversement, supposons M' et M'' noethériens. Soit N un sous-module de M, alors $v(N)$ est de type fini : $v(N) = \sum_{1 \le i \le r} Av(x_i)$ avec $x_i \in N$. Soit $N_1 = \sum_{1 \le i \le r} Ax_i$, c'est un sous-module de N de type fini et l'on voit, en appliquant v, que

$$N = N_1 + N \cap \mathrm{Ker}(v) = N_1 + N \cap \mathrm{Im}(u) \ ,$$

donc N est de type fini. □

Une des applications importantes de cette proposition est le résultat suivant.

Proposition 7.1.5. *Soient A un anneau noethérien et M un A-module. Alors M est un A-module noethérien si et seulement si c'est un A-module de type fini.*

Démonstration. La condition est nécessaire, de manière évidente. Supposons M de type fini, $M = \sum_{1 \leq i \leq r} Ax_i$. La surjection $A^r \to M$ qui à $(a_1, \cdots, a_r)$ associe $\sum_{1 \leq i \leq r} a_i x_i$ montre qu'il suffit de prouver que A^r est noethérien. Cela se fait par récurrence sur r, à l'aide de la suite exacte (et de la proposition précédente)

$$0 \to A^{r-1} \overset{\mathrm{u}}{\to} A^r \overset{\mathrm{v}}{\to} A \to 0$$

où u et v sont définis par :

$$\mathrm{u}(a_1, \cdots, a_{r-1}) = (a_1, \cdots, a_{r-1}, 0) \quad , \quad \mathrm{v}(a_1, \cdots, a_r) = a_r.$$

□

7.2 Intégralité

7.2.1 Éléments entiers sur un anneau

Théorème 7.2.1. *Soient $A \subseteq B$ un anneau et un sous-anneau, soit $x \in B$. Les assertions suivantes sont équivalentes :*
(i) il existe un polynôme $P(X)$ de $A[X]$, unitaire, tel que $P(x) = 0$;
(ii) le A-module $A[x]$ est de type fini ;
(iii) il existe un $A[x]$-module fidèle, M, qui est aussi un A-module de type fini.

Rappelons que $A[x]$ désigne le sous-anneau de B engendré par A et x et qu'un $A[x]$-module M est fidèle si, étant donné $\lambda \in A[x]$, $\lambda m = 0$ pour tout $m \in M$ implique $\lambda = 0$.

Démonstration. (i) implique (ii) est immédiat, pour (ii) implique (iii) il suffit de choisir $M = A[x]$. Montrons que (iii) implique (i).

On écrit $M = \sum_{1 \leq i \leq r} A\omega_i$ et $x\omega_i = \sum_{1 \leq j \leq r} a_{j,i}\omega_j$ avec $a_{j,i} \in A$, $1 \leq i, j \leq r$. Dans l'anneau des matrices carrées $r \times r$ à coefficients dans $A[x]$, on pose

$$\mathcal{M} = (a_{j,i}) - xI_r$$

(I_r est la matrice identité). On a

$$\mathcal{M} \cdot \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad .$$

Soit $\mathcal{M}'$ la matrice des cofacteurs de $\mathcal{M}$, on a aussi

$$\mathcal{M}' \cdot \mathcal{M} = (\det\mathcal{M}) \cdot I.$$

Il vient

$$(\det\mathcal{M}) \cdot I \cdot \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \mathcal{M}' \cdot \mathcal{M} \cdot \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} .$$

On a donc que $(\det\mathcal{M})m = 0$ pour tout m appartenant à M. Le $A[x]$-module M étant fidèle, il suit $\det\mathcal{M} = 0$ et ceci donne la relation cherchée. □

Définition 7.2.2. Soient $A \subseteq B$ un anneau et un sous-anneau. Un élément x de B qui vérifie l'une de ces propriétés équivalentes du théorème 7.2.1 est dit *entier sur* A.

L'anneau B est dit *entier sur* A si tous ses éléments sont entiers sur A. L'ensemble des éléments de B entiers sur A s'appelle la *fermeture intégrale de* A *dans* B. Un anneau A intègre est dit *intégralement clos* s'il est égal à sa fermeture intégrale dans son corps des fractions. Soit $\varphi : A \to B$ un morphisme d'anneaux, on dit qu'il est *entier* si B est entier sur $\varphi(A)$.

Proposition 7.2.3. *Soient $A \subseteq B$ un anneau et un sous anneau.*
(i) Soient $x_1, \cdots, x_r$ des éléments de B, entiers sur A, alors l'anneau $A[x_1, \cdots, x_r]$ est un A-module de type fini et est donc entier sur A.
(ii) La fermeture intégrale de A dans B est un anneau.
(iii) Soit C un anneau admettant B en tant que sous-anneau (donc $A \subseteq B \subseteq C$ sont des anneaux et des sous-anneaux); si B est entier sur A et C est entier sur B, alors C est entier sur A.

Démonstration. (i) Si un élément x de B est racine du polynôme unitaire $P(X) \in A[X]$, de degré d, alors on voit que tous les x^n, $n \geq d$ sont des combinaisons linéaires à coefficients dans A des x^i, $0 \leq i \leq d-1$. Ceci montre que $A[x_1, \cdots, x_r]$ est un A-module de type fini. Enfin, on voit que tout élément x de $A[x_1, \cdots, x_r]$ est entier sur A car $A[x_1, \cdots, x_r]$ est un $A[x]$-module fidèle du fait que c'est un anneau unitaire.

(ii) Soient x et y appartenant à B, entiers sur A. Il faut prouver que $x+y$ et xy sont entiers sur A. Ceci vient du fait que, d'après (i), $A[x, y]$ est entier sur A.

(iii) Soit $x \in C$ et soit $x^d + b_1 x^{d-1} + \cdots + b_d = 0$ une relation de dépendance intégrale de x sur B, avec donc $b_1, \cdots, b_d$ dans B. Alors x est entier sur $A[b_1, \cdots, b_d]$ et ce dernier est un A-module de type fini d'après (i), donc $A[x, b_1, \cdots, b_d]$ est un A-module de type fini et un $A[x]$-module fidèle. □

Remarque 7.2.4. Soient A un anneau intègre, $K = \mathrm{Frac}(A)$, L une extension algébrique de K et B la fermeture intégrale de A dans L. Alors B est intégralement clos et $\mathrm{Frac}(B) = L$. En fait, si $S = A - \{0\}$ (c'est une partie

multiplicativement fermée de B) on a $L = S^{-1}B$. En effet, soient $x \in L$ et $\mathrm{irr}(x, K; X) = X^d + (a_1/b)x^{d-1} + \cdots + (a_d/b)$ avec $a_1, \cdots, a_d, b \in A$. On a $bx \in B$.

Remarque 7.2.5. Soient $A \subseteq B$ un anneau et un sous-anneau avec B entier sur A. Soit S une partie multiplicativement fermée de A (donc de B). Alors, $S^{-1}B$ est entier sur $S^{-1}A$.

Cette dernière remarque est laissée en exercice. On ne connaît sans doute la définition des anneaux de fractions que dans le cas intègre, le cas général est introduit au paragraphe 3.1 de ce chapitre.

7.2.2 Quelques propriétés des anneaux intégralement clos

Proposition 7.2.6. *Soit A un anneau factoriel, alors A est intégralement clos.*

Démonstration. Soit $K = \mathrm{Frac}(A)$ et soit $a/b \in K$, entier sur A, avec $a, b \in A$ et $\mathrm{pgcd}(a, b) = 1$. On a donc une relation

$$(\frac{a}{b})^n + \lambda_1(\frac{a}{b})^{n-1} + \cdots + \lambda_n = 0$$

avec $\lambda_i \in A$; il vient

$$a^n + \lambda_1 a^{n-1}b + \cdots + \lambda_n b^n = 0$$

dont il résulte que tout diviseur irréductible de b divise a, donc $b \in A^*$. □

Proposition 7.2.7. *Soient A un anneau intégralement clos, $K = \mathrm{Frac}(A)$, L une extension de K et $x \in L$ entier sur A. Alors* $\mathrm{irr}(x, K; X)$ *appartient à $A[X]$.*

Démonstration. Soit $P(X) \in A[X]$, unitaire, tel que $P(x) = 0$. On a $\mathrm{irr}(x, K; X)$ qui divise $P(X)$ dans $K[X]$, donc tous les conjugués de x (dans un corps algébriquement clos convenable) sont entiers sur A ; les fonctions symétriques des racines montrent alors que les coefficients de $\mathrm{irr}(x, K; X)$ sont entiers sur A, et ce sont des éléments de K... □

Proposition 7.2.8. *Soient A un anneau noethérien et intégralement clos, $K = \mathrm{Frac}(A)$, L une extension séparable finie de K et B la fermeture intégrale de A dans L. Alors B est un A-module de type fini (c'est donc un anneau noethérien).*

Démonstration. Soit $x \in L$, alors il existe $d \in A - \{0\}$ tel que $dx \in B$, en effet, il suffit de choisir un dénominateur commun aux coefficients de $\mathrm{irr}(x, K; X)$.

Donc il existe une base $\{\omega_1, \cdots, \omega_n\}$ de L sur K formée d'éléments de B. Soit $B' = \oplus_{1\leq i\leq n} A\omega_i$, on a $B' \subseteq B$. Soit

$$C = \{x \in L \ / \ \mathrm{Tr}_{L/K}(xy) \in A \ \forall y \in B'\}.$$

On voit que $B \subseteq C$ et que $C = \oplus_{1\leq i\leq n} A\omega_i^*$, $\{\omega_i^*\}_{1\leq i\leq n}$ désignant la base duale par rapport à la forme bilinéaire $L \times L \to K$ qui à (x, y) associe $\mathrm{Tr}_{L/K}(xy)$. Donc $B \subseteq \oplus_{1\leq i\leq n} A\omega_i^*$. Il vient que B est de type fini sur A. □

7.2.3 Sur quelques fermetures intégrales

L'objet de ce paragraphe est de donner quelques propriétés des fermetures intégrales de $\mathbb{Z}$ (resp. $\mathbb{F}_q[T]$) dans les extensions finies de $\mathbb{Q}$ (resp. $\mathbb{F}_q(T)$). Remarquons, grâce aux propositions 7.2.6 et 7.2.8, que si L est une extension finie de $\mathbb{Q}$ (resp. une extension finie *séparable* de $\mathbb{F}_q(T)$), on sait déjà que ces fermetures intégrales sont des anneaux noethériens de type fini sur $\mathbb{Z}$ (resp. $\mathbb{F}_q[T]$). Nous allons compléter ce résultat.

Lemme 7.2.9. *Soient A un anneau principal et M un A-module de type fini et sans torsion, alors M est un A-module libre.*

Démonstration. Soit $\mathcal{M}$ l'ensemble des sous-A-modules de M qui sont libres. On a $\mathcal{M} \neq \emptyset$ car $Ax \in \mathcal{M}$ pour tout $x \in M - \{0\}$ du fait que M est sans torsion. Soit M_0 un élément de $\mathcal{M}$ maximal (M est noethérien). Montrons que $M_0 = M$.

Supposons $M_0 \neq M$ et soit $\omega \in M - M_0$. Posons $M_0 = \oplus_{1\leq i\leq n} A\omega_i$. Alors $M_0 + A\omega$ n'est pas un A-module libre, $\{\omega_1, \cdots, \omega_n, \omega\}$ est lié sur A, donc

$$I = \{a \in A \ / \ a\omega \in M_0\} \ \neq \ \{0\}.$$

On voit aussi que I est un idéal de A, donc il s'écrit $I = aA$. Soit p un diviseur irréductible de a (p existe car $I \neq A$ du fait que $\omega \notin M_0$). Ecrivons $a = a'p$, quitte à changer ω en $a'\omega$, on peut supposer que $I = pA$ avec p irréductible ; donc I est un idéal maximal de A.

Ecrivons

$$(\star) \qquad p\omega + \lambda_1\omega_1 + \cdots + \lambda_n\omega_n = 0$$

avec les $\lambda_i \in A$. Comme $\omega \notin M_0$, p ne divise pas tous les λ_i ; on peut supposer que p ne divise pas λ_1. Soient donc $l, k \in A$ tels que $l\lambda_1 = 1 + kp$ (λ_1 est inversible modulo p) et soit

$$M_1 = A(l\omega + k\omega_1) + A\omega_2 + \cdots + A\omega_n.$$

Montrons que M_1 est libre sur A. Soient en effet $a_1, \cdots, a_n \in A$ tels que

$$(\star\star) \qquad a_1(l\omega + k\omega_1) + a_2\omega_2 + \cdots + a_n\omega_n = 0.$$

Cette dernière formule implique que $a_1 l\omega \in M_0$, donc que $a_1 \in I = pA$ puisque l est premier avec p. Posons $a_1 = a_1' p$, il suit alors de $(\star\star)$ et de l'expression de $p\omega$ donnée par $(\star)$ que

$$a_1'(pk - l\lambda_1)\omega_1 + (a_2 - a_1' l\lambda_2)\omega_2 + \cdots + (a_n - a_1' l\lambda_n)\omega_n = 0.$$

Comme $pk - l\lambda_1 = -1$, il vient que $a_1' = a_2 = \cdots = a_n = 0$.

Montrons que $M_0 \subseteq M_1$. De $(\star)$ il vient

$$pl\omega + l\lambda_1\omega_1 + \cdots + l\lambda_n\omega_n = 0,$$

donc, puisque $l\lambda_1 = 1 + kp$

$$\omega_1 = -p(l\omega + k\omega_1) - l\lambda_2\omega_2 - \cdots - l\lambda_n\omega_n \in M_1.$$

Montrons $M_0 \neq M_1$. Si $M_0 = M_1$, alors $l\omega \in M_0$, par suite (cf $(\star)$)

$$\omega = (l\lambda_1 - kp)\omega \in M_0$$

ce qui est faux.

Ainsi M_1 est libre sur A et contient strictement M_0. Ceci prouve que ω n'existe pas. □

Ce lemme avec 7.2.8 donne, pour le extensions finies de $\mathbb{Q}$, les résultats que nous cherchions :

Proposition 7.2.10. *Soient A un anneau principal, $K = \mathrm{Frac}(A)$, L une extension séparable finie de K et B la fermeture intégrale de A dans L. Alors B est un A-module libre de type fini (ses bases ont pour cardinal $[L : K]$).*

Le cas des extensions finies de $\mathbb{F}_q(T)$ demande des arguments supplémentaires.

Proposition 7.2.11. *Soient $\mathbb{F}_q$ un corps fini de caractéristique p, $K = \mathbb{F}_q(T)$, $A = \mathbb{F}_q[T]$, L une extension algébrique finie de K et B la fermeture integrale de A dans L. Alors B est un A-module libre de type fini (ses bases ont pour cardinal $[L : K]$).*

Démonstration. La preuve de cette proposition consiste à montrer que B est de type fini sur A (cf le lemme 7.2.9). On commence par étudier le cas des extensions purement inséparables.

Le cas où L/K est purement inséparable. Soit $p^r = [L : K]$. Notons que, pour tout $x \in L$, on a $x^{p^r} \in K$ et que si $x \in B$ alors $x^{p^r} \in A$ (le polynôme $\mathrm{irr}(x, K; X)$ est dans $A[X]$, cf. 7.2.7, il est de la forme $X^{p^\alpha} - x^{p^\alpha}$ avec $\alpha \leq r$). Il suit que pour tout x appartenant à B, x^{q^r} appartient à A.

Soient A^{q^r} (resp. B^{q^r}) l'ensemble des puissances q^r-ièmes des éléments de A (resp. B). On a

$$A^{q^r} = \mathbb{F}_q[T^{q^r}] \quad \text{et} \quad A^{q^r} \subset B^{q^r} \subset A.$$

Comme A est un A^{q^r}-module de type fini, il vient que B^{q^r} est lui aussi un A^{q^r}-module de type fini. Il en résulte facilement que B est un A-module de type fini.

Fin de la démonstration. Soit L_1 une fermeture normale de L/K (dans une clôture algébrique L^{alg} de L) et soit B_1 la fermeture intégrale de A (donc de B) dans L_1. Il suffit de prouver que B_1 est de type fini sur A, car, si tel est le cas, B_1 sera un A-module noethérien et B en est un sous-module.

Soit $G = \text{Gal}(L_1/K)$. L'extension se décompose en

$$K \to L_1^G \to L_1.$$

Soit B' la fermeture intégrale de A dans L_1^G. Comme L_1^G/K est finie et purement inséparable, B' est de type fin sur A. Comme l'extension L_1/L_1^G est finie et séparable, B_1, qui est la fermeture intégrale de B' dans L_1, est de type fini sur B' (cf. 7.2.8).

On a donc prouvé que B est de type fini sur A. □

7.3 Idéaux premiers

7.3.1 Les anneaux de fractions

Théorème 7.3.1. *Soient A un anneau (commutatif, unitaire, non nécessairement intègre) et S une partie de A multiplicativement fermée (i.e. $1 \in S$, $0 \notin S$ et $s, s' \in S \Rightarrow ss' \in S$). Alors il existe un couple $(\theta, S^{-1}A)$ où $S^{-1}A$ est un anneau et $\theta : A \to S^{-1}A$ un homomorphisme d'anneaux possédant les propriétés suivantes :*
(i) $\theta(S) \subset (S^{-1}A)^*$,
(ii) pour tout couple (β, B) où B est un anneau et $\beta : A \to B$ est un homomorphisme tel que $\beta(S) \subset B^*$, il existe un unique homomorphisme $\varphi : S^{-1}A \to B$ tel que $\varphi \circ \theta = \beta$.

Le couple $(\theta, S^{-1}A)$ est unique à isomorphisme près.

Démonstration. Sur $S \times A$ on considère la relation :

$$(s, a) \sim (s', a') \Leftrightarrow \exists\ t \in S\ /\ t(sa' - s'a) = 0$$

Remarquer que la différence avec le cas intègre est l'existence de t. On vérifie que $\sim$ est une relation d'équivalence compatible avec les lois suivantes sur $S \times A$:

$$(s, a) + (s', a') = (ss', sa' + s'a)\ ,\ (s, a)(s', a') = (ss', aa').$$

Alors $S^{-1}A = S \times A/\sim$ est un anneau unitaire (d'unité la classe de $(1, 1)$), $\theta : A \to S^{-1}A$ qui a $a \in A$ associe la classe de $(1, a)$ est un homomorphisme d'anneaux, les éléments de $\theta(S)$ sont inversibles (car $(s, 1)(1, s) = (s, s)$ est dans la classe de $(1, 1)$), de plus, la classe de (s, a) s'écrit $\theta(s)^{-1}\theta(a)$. Etant

donné (β, B) comme dans l'énoncé, alors $\varphi : \theta(s)^{-1}\theta(a) \mapsto \beta(s)^{-1}\beta(a)$ est l'application cherchée.

Montrons l'unicité. Soient deux couples, (θ, C) et (θ', C'), possédant les propriétés (i) et (ii) de l'énoncé. Soient $\varphi : C \to C'$ et $\varphi' : C' \to C$ donnés par (ii). On a donc

$$\varphi' \circ \varphi \circ \theta = \varphi' \circ \theta' = \theta,$$

mais on a aussi $\mathrm{id}_C \circ \theta = \theta$; il suit donc de l'unicité affirmée dans (ii) que $\mathrm{id}_C = \varphi' \circ \varphi$. On montre de même que $\mathrm{id}_{C'} = \varphi \circ \varphi'$. □

Définition 7.3.2. Soient A un anneau (commutatif, unitaire, non nécessairement intègre) et S une partie de A multiplicativement fermée. Le couple $(\theta, S^{-1}A)$ (ou encore $S^{-1}A$) donné par le théorème 7.3.1 est appelé anneau des fractions de A de dénominateurs dans S.

Remarque 7.3.3. L'application θ n'est pas en général injective : $ker(\theta)$ est l'ensemble des éléments de A qui divisent zéro avec un élément de S.

Exemple 7.3.4. Soient n et m deux entiers premiers entre eux, soit S la partie multiplicativement fermée de $A = \mathbf{Z}/nm\mathbf{Z}$ engendrée par la classe de m, alors $S^{-1}A \simeq \mathbf{Z}/n\mathbf{Z}$.

Les liens entre les idéaux premiers de $S^{-1}A$ et ceux de A sont les mêmes que dans le cas intègre, les abus de notations aussi (on n'écrit pas l'application θ). Le lemme suivant sera utile plus loin.

Lemme 7.3.5. *Soient A un anneau, I un idéal de A, S une partie de A multiplicativement fermée. On suppose que $I \cap S = \emptyset$. Alors il existe un idéal premier $\mathfrak{P}$ de A contenant I et ne rencontrant pas S.*

Démonstration. Soit $\mathcal{I}$ l'ensemble des idéaux de A contenant I et ne rencontrant pas S, $\mathcal{I}$ est non vide car $I \in \mathcal{I}$. C'est un ensemble ordonné inductif pour l'inclusion, donc (théorème de Zorn) il possède un plus grand élément $\mathfrak{P}$. Montrons que $\mathfrak{P}$ est premier. Sinon, il existe $a, b \in A$ avec $a \notin \mathfrak{P}$, $b \notin \mathfrak{P}$, $ab \in \mathfrak{P}$; les idéaux $\mathfrak{P}+aA$ et $\mathfrak{P}+bA$ contiennent $\mathfrak{P}$ et en sont distincts, donc il existe $p_1, p_2 \in \mathfrak{P}$, $c_1, c_2 \in A$, $s_1, s_2 \in S$ tels que $s_1 = p_1 + ac_1$, $s_2 = p_2 + bc_2$. On a $s_1 s_2 = p_1 p_2 + ac_1 p_2 + bc_2 p_1 + abc_1 c_2 \in \mathfrak{P}$, d'où la contradiction. □

7.3.2 A propos des modules de type fini

Lemme 7.3.6. *(Lemme de Nakayama) Soient A un anneau, I son radical (on dit aussi le radical de Jacobson, il s'agit de l'intersection des idéaux maximaux de A) et $\mathfrak{A}$ un idéal de A contenu dans I. Soit M un A-module de type fini. Alors la relation $\mathfrak{A}M = M$ implique $M = (0)$.*

Démonstration. On écrit $M = \sum_{i=1}^{r} Ax_i$ avec r minimal (et $x_i \in M$). La relation $\mathfrak{A}M = M$ implique qu'il existe des $a_i \in \mathfrak{A}$ tel que $x_1 = \sum_{i=1}^{r} a_i x_i$,

donc $(1-a_1)x_1 = \sum_{i=2}^{r} a_i x_i$, mais $1-a_1$ n'est dans aucun idéal maximal de A, donc est dans A^*. Ceci contredit la minimalité de r. Donc r n'existe pas. □

Corollaire 7.3.7. *Les hypothèses sont les mêmes qu'en 7.3.6 . Soit de plus N un sous module de M. Alors la relation $M = \mathfrak{A}M + N$ implique $M = N$.*

La preuve se fait en considérant M/N.

7.3.3 Prolongements des idéaux premiers

Théorème 7.3.8. *(Cohen-Seidenberg) Soient $A \subseteq B$ un anneau et un sous-anneau ; on suppose que B est entier sur A. Soit $\mathfrak{P}$ un idéal premier de A. Alors il existe un idéal premier $\mathfrak{Q}$ de B au dessus de $\mathfrak{P}$ (i.e. tel que $\mathfrak{Q} \cap A = \mathfrak{P}$), de plus, $\mathfrak{P}$ est maximal si et seulement si $\mathfrak{Q}$ l'est.*

Démonstration. Existence de $\mathfrak{Q}$. Soit $S = A - \mathfrak{P}$, c'est une partie multiplicativement fermée de A et $S^{-1}A$, qui se note $A_{\mathfrak{P}}$, est un anneau local d'idéal maximal $\mathfrak{P}A_{\mathfrak{P}}$. Compte tenu du lemme 7.3.5, il faut montrer que $\mathfrak{P}B \cap S = \emptyset$. Sinon il existe $s \in S$, $p_1, ..., p_r \in \mathfrak{P}$, $b_1, ..., b_r \in B$ tels que

$$(\star) \qquad s = p_1 b_1 + ... + p_r b_r$$

Soit $C = A_{\mathfrak{P}}[b_1, ..., b_r] \subseteq S^{-1}B$. On voit que l'anneau C est un $A_{\mathfrak{P}}$-module de type fini tel que, à cause de $(\star)$, $1 \in \mathfrak{P}A_{\mathfrak{P}}C$, donc $C = \mathfrak{P}A_{\mathfrak{P}}C$. Il vient $C = (0)$ (Nakayama), ce qui est faux $(1 \in C)$.

Montrons que $\mathfrak{P}$ est maximal si et seulement $\mathfrak{Q}$ l'est. L'inclusion $A \subset B$ et les deux surjections canoniques $A \to A/\mathfrak{P}$, $B \to B/\mathfrak{Q}$ donnent, par factorisation, un morphisme injectif $u : A/\mathfrak{P} \to B/\mathfrak{Q}$. Ainsi le lemme suivant permet de conclure.

Lemme 7.3.9. *Soient $F \subseteq E$ un anneau et un sous-anneau. On suppose E intègre et entier sur F. Alors F est un corps si et seulement s'il en est de même de E.*

Démonstration. Si F est un corps. Soit $x \in E$, $x \neq 0$, $x^d + a_1 x^{d-1} + \cdots + a_d = 0$ avec $a_i \in F$ et $a_d \neq 0$ (ceci est possible car E est intègre). Il vient $x(x^{d-1} + a_1 x^{d-2} + \cdots + a_{d-1})(-1/a_d) = 1$, donc $x \in E^*$.

Si E est un corps. Soit $x \in F$, $x \neq 0$; $1/x \in E$ donc on a une relation du type $(1/x)^d + a_1(1/x)^{d-1} + \cdots + a_d = 0$ avec $a_i \in F$. Il vient $1 + a_1 x + \cdots + a_d x^d = 0$, donc $1 = (-a_1 - \cdots - a_d x^{d-1})x$, par suite $1/x \in F$. □

7.3.4 Le cas des extensions algébriques

Théorème 7.3.10. *Soient K une extension algébrique finie de $\mathbb{Q}$ (resp. $\mathbb{F}_q(T)$), L une extension algébrique finie de K, A la fermeture intégrale de $\mathbb{Z}$ (resp. $\mathbb{F}_q[T]$) dans K, B celle de A dans L (donc de $\mathbb{Z}$, resp. $\mathbb{F}_q[T]$, dans*

L). Soit $\mathfrak{P}$ un idéal premier non nul de A (donc $\mathfrak{P}$ est maximal) et soit $\mathfrak{I}_\mathfrak{P}$ l'ensemble des idéaux premiers de B au dessus de $\mathfrak{P}$. Alors $\mathfrak{I}_\mathfrak{P}$ est non vide, fini, formé d'idéaux maximaux ; de plus, $\mathfrak{I}_\mathfrak{P}$ est égal à l'ensemble des idéaux premiers de B contenant l'idéal $\mathfrak{P}B$ de B.

Démonstration. On va prouver que $\mathfrak{I}_\mathfrak{P}$ est égal à l'ensemble des idéaux premiers de B contenant l'idéal $\mathfrak{P}B$ de B et que ce dernier ensemble est fini. Cela suffit, compte tenu des résultats précédents.

Lemme 7.3.11. *Dans un anneau noethérien tout idéal radiciel est égal à une intersection finie d'idéaux premiers (un idéal I est radiciel si $I = \sqrt{I}$).*

Démonstration de 7.3.11. Soient A un anneau noethérien et $\mathfrak{I}$ la famille de ses idéaux radiciels qui ne sont pas intersections finies d'idéaux premiers. Supposons $\mathfrak{I} \neq \emptyset$. Soit alors I un élément maximal de $\mathfrak{I}$. L'idéal I n'est pas premier : il existe $a, b \in A$ tels que $a \notin I$, $b \notin I$ et $ab \in I$. Les idéaux $\sqrt{I + aA}$ et $\sqrt{I + bA}$ contiennent I mais en sont distincts, ils sont donc égaux à des intersections finies d'idéaux premiers. La contradiction vient alors de :

$$\sqrt{I + aA} \cap \sqrt{I + bA} = \sqrt{(I + aA)(I + bA)} = \sqrt{I} = I.$$

Corollaire 7.3.12. *Soient A un anneau noethérien et I l'un de ses idéaux. Alors les idéaux premiers contenant I, minimaux pour ces propriétés, forment un ensemble fini et $\sqrt{I}$ est égal à leur intersection.*

Démonstration de 7.3.12. Il faut montrer que si $\mathfrak{P}$, $\mathfrak{P}_1$,..., $\mathfrak{P}_r$ sont des idéaux premiers de A, que si $\mathfrak{P} \supset \cap_{1 \leq i \leq r} \mathfrak{P}_i$, alors il existe i tel que $\mathfrak{P} \supset \mathfrak{P}_i$. Sinon, pour tout i, il existe $x_i \in \mathfrak{P}_i$ tel que $x_i \notin \mathfrak{P}$, on a $x_1 \cdots x_r \in \cap_{1 \leq i \leq r} \mathfrak{P}_i \subset \mathfrak{P}$, d'où la contradiction.

Fin de la démonstration du théorème 7.3.10. Un idéal $\mathfrak{Q}$ premier de B, minimal parmi ceux contenant $\mathfrak{P}B$, vérifie $(\mathfrak{Q} \cap A) \supset \mathfrak{P}$, donc $(\mathfrak{Q} \cap A) = \mathfrak{P}$ puisque $\mathfrak{P}$ est maximal. De plus, comme tout idéal premier de B non nul est maximal (cf la remarque suivante), tout idéal premier de B contenant $\mathfrak{P}B$ est minimal parmi ceux contenant $\mathfrak{P}B$. □

Remarque 7.3.13. Soient K une extension finie de $\mathbb{Q}$ (resp. $\mathbb{F}_q(T)$, où $\mathbb{F}_q$ est un corps fini à q éléments) et A la fermeture intégrale de $\mathbb{Z}$ ou $\mathbb{F}_q[T]$ dans K. Alors tout idéal premier non nul de A est maximal. En effet, étant donné un idéal $I \neq \{0\}$ de A, on a $I \cap \mathbb{Z} \neq \{0\}$ (resp. $I \cap \mathbb{F}_q[T] \neq \{0\}$) car par exemple $I \cap \mathbb{Z}$ (resp. $I \cap \mathbb{F}_q[T]$) contient le terme constant du polynôme minimal de tout élément non nul de I. Donc, tout idéal premier non nul de A est au dessus d'un idéal premier non nul de $\mathbb{Z}$ (resp. $\mathbb{F}_q[T]$), il est donc maximal (théorème de Cohen-Seidenberg).

7.4 Idéaux premiers et extensions galoisiennes

Dans tout ce paragraphe, K est une extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_q(T)$ ($\mathbb{F}_q$ est un corps fini à q éléments) et A est la fermeture intégrale de $\mathbb{Z}$ ou $\mathbb{F}_q[T]$ dans K ; le corps L est une extension galoisienne finie de K et B est la fermeture intégrale de A dans L. On sait que A et B sont des modules (libres) de type fini sur $\mathbb{Z}$ ou $\mathbb{F}_q[T]$, il en résulte que leurs quotients par leurs idéaux maximaux sont des corps finis. On pose

$$G = \mathrm{Gal}(L/K).$$

7.4.1 Groupes de décomposition

Proposition 7.4.1. *Soient $\mathfrak{p}$ un idéal maximal de A et $\mathcal{I}_\mathfrak{p}$ l'ensemble des idéaux maximaux de B au dessus de $\mathfrak{p}$. Alors, G agit transitivement sur $\mathcal{I}_\mathfrak{p}$ (i.e. G agit sur $\mathcal{I}_\mathfrak{p}$ et pour tous $\mathfrak{P}$ et $\mathfrak{Q}$ dans $\mathcal{I}_\mathfrak{p}$ il existe σ appartenant à G tel que $\sigma(\mathfrak{P}) = \mathfrak{Q}$).*

Démonstration. Le fait que G opère sur $\mathcal{I}_\mathfrak{p}$ est immédiat. Soient $\mathfrak{P}$ et $\mathfrak{Q}$ appartenant à $\mathcal{I}_\mathfrak{p}$ tels que $\mathfrak{Q} \neq \sigma(\mathfrak{P})$ pour tout $\sigma \in G$. Le théorème des restes chinois affirme l'existence de $x \in B$ tel que

$x \equiv 0$ mod. $\mathfrak{Q}$,

$x \equiv 1$ mod. $\sigma(\mathfrak{P})$ pour tout $\sigma \in G$.

Alors la première relation montre que $N_{L/K}(x) \in \mathfrak{Q} \cap A = \mathfrak{p}$ tandis que la seconde montre que $N_{L/K}(x) \notin \mathfrak{P}$, donc $N_{L/K}(x) \notin \mathfrak{P} \cap A = \mathfrak{p}$, ce qui donne une contradiction. □

Définition 7.4.2. Soient $\mathfrak{p}$ un idéal maximal de A et $\mathfrak{P}$ un idéal maximal de B au dessus de $\mathfrak{p}$. Soit $G_\mathfrak{P}$ l'ensemble des σ de G tels que $\sigma(\mathfrak{P}) = \mathfrak{P}$; c'est un sous-groupe de G appelé le *groupe de décomposition de* $\mathfrak{P}$. Remarquons que, pour tout $\sigma \in G$, on a $G_{\sigma(\mathfrak{P})} = \sigma G \sigma^{-1}$. Il est facile de vérifier que l'on a un morphisme canonique

$$r_\mathfrak{P} : G_\mathfrak{P} \to \mathrm{Gal}(B/\mathfrak{P}, A/\mathfrak{p})$$

qui, la surjection canonique $B \to B/\mathfrak{P}$ étant désignée par un surlignage, à $\sigma \in G_\mathfrak{P}$ associe $\overline{x} \to \overline{\sigma(x)}$. Dans la définition de $r_\mathfrak{P}$, comme dans ce qui suit, on confond avec une inclusion l'homomorphisme canonique $A/\mathfrak{p} \to B/\mathfrak{P}$ venant par factorisation de $A \subseteq B$.

Théorème 7.4.3. *Soient $\mathfrak{p}$ un idéal maximal de A, $\mathfrak{P}$ un idéal maximal de B au dessus de $\mathfrak{p}$. Alors l'homomorphisme canonique*

$$r_\mathfrak{P} : G_\mathfrak{P} \to \mathrm{Gal}(B/\mathfrak{P}, A/\mathfrak{p})$$

est surjectif.

La démonstration nécessite deux autres résultats, qui sont intéressants en soi.

Proposition 7.4.4. *Soient $\mathfrak{P}$ un idéal maximal de B, $G_{\mathfrak{P}}$ le groupe de décomposition de $\mathfrak{P}$, $L^{\mathfrak{P}}$ le sous-corps de L des éléments invariants sous $G_{\mathfrak{P}}$ et $B^{\mathfrak{P}} = B \cap L^{\mathfrak{P}}$ la fermeture intégrale de A dans $L^{\mathfrak{P}}$. Alors, au dessus de l'idéal premier $\mathfrak{Q} = \mathfrak{P} \cap B^{\mathfrak{P}}$ de $B^{\mathfrak{P}}$, il n'y a qu'un seul idéal premier de B, qui est $\mathfrak{P}$.*

Démonstration. On a d'après la correspondance de Galois $G_{\mathfrak{P}} = \mathrm{Gal}(L, L^{\mathfrak{P}})$. Il suit de 7.4.1 que $G_{\mathfrak{P}}$ agit transitivement sur les idéaux premiers de B au dessus de $\mathfrak{Q}$ et l'un d'entre eux est $\mathfrak{P}$. □

Proposition 7.4.5. *Soient $\mathfrak{p}$ un idéal maximal de A, $\mathfrak{P}$ un idéal maximal de B au dessus de $\mathfrak{p}$, $G_{\mathfrak{P}}$ le groupe de décomposition de $\mathfrak{P}$, $L^{\mathfrak{P}}$ le sous-corps de L des éléments invariants sous $G_{\mathfrak{P}}$, $B^{\mathfrak{P}} = B \cap L^{\mathfrak{P}}$ la fermeture intégrale de A dans $L^{\mathfrak{P}}$ et $\mathfrak{Q} = \mathfrak{P} \cap B^{\mathfrak{P}}$. Alors l'inclusion*

$$A/\mathfrak{p} \hookrightarrow B^{\mathfrak{P}}/\mathfrak{Q}$$

(qui est en fait l'injection canonique obtenue par factorisation de $A \subseteq B^{\mathfrak{P}}$) est une égalité.

Démonstration. Soit $x \in B^{\mathfrak{P}}$. Montrons
($\star$) il existe $y \in B^{\mathfrak{P}}$ tel que
$y \equiv x$ mod. $\mathfrak{Q}$ et
$\sigma(y) \equiv 1$ mod. $\mathfrak{Q}$ pour tout $\sigma \notin G_{\mathfrak{P}}$ ($\sigma \in G$).
Ceci étant prouvé, on voit facilement que

$$N_{L^{\mathfrak{P}}/K}(y) \equiv x \text{ mod. } \mathfrak{Q},$$

ce qui donne la proposition. Prouvons ($\star$).

Soit $\sigma \in G - G_{\mathfrak{P}}$, à cause de 7.4.2, l'idéal premier $\mathfrak{Q}_\sigma = \sigma^{-1}(\mathfrak{P}) \cap B^{\mathfrak{P}}$ n'est pas égal à $\mathfrak{Q}$, d'où l'existence de $y \in B^{\mathfrak{P}}$ tel que
$y \equiv x$ mod. $\mathfrak{Q}$,
$y \equiv 1$ mod. $\mathfrak{Q}_\sigma$ pour tout $\sigma \in G - G_{\mathfrak{P}}$.
Ceci implique ($\star$). □

Démonstration du théorème 7.4.3. On utilise les notations des deux propositions précédentes. La dernière de ces propositions montre qu'il suffit de prouver le théorème lorsque $K = L^{\mathfrak{P}}$, ce que l'on suppose dorénavant. Soient $\overline{A} = A/\mathfrak{p}$, $\overline{B} = B/\mathfrak{P} = \overline{A}(\overline{x})$ avec $x \in B$ ($\overline{B}$ est un corps fini, donc séparable sur $\overline{A}$). Soit $f(X) = \mathrm{irr}(x, K; X)$, on a $f(X) \in A[X]$ et $\overline{f}(X)$ (l'image canonique de $f(X)$ dans $\overline{A}[X]$) est divisible par $g(X) = \mathrm{irr}(\overline{x}, \overline{A}; X)$ dans $\overline{A}[X]$. Soit $\sigma \in \mathrm{Gal}(\overline{B}, \overline{A})$, alors σ est complètement déterminé par $\sigma(\overline{x})$ et, puisque $g(X)$ divise $\overline{f}(X)$ dans $\overline{A}[X]$, il existe une racine y de $f(X)$ dans B telle que $\overline{y} = \sigma(\overline{x})$. Il existe τ appartenant à $\mathrm{Hom}_K(K(x), L)$ tel que $\tau(x) = y$. Alors, tout prolongement de τ à L est un antécédent de σ par $r_{\mathfrak{P}}$. □

7.4.2 Applications

Le théorème 7.4.3 admet le corollaire suivant

Corollaire 7.4.6. *Soient $\mathfrak{p}$ un idéal maximal de A, $\mathfrak{P}$ un idéal maximal de B au dessus de $\mathfrak{p}$, $G_{\mathfrak{P}}$ le groupe de décomposition de $\mathfrak{P}$. On suppose que $L = K(x)$ avec $x \in B$ et que $f(X) = irr(x, K; X)$ (qui appartient à $A[X]$) est tel que son image canonique dans $A/\mathfrak{p}[X]$ est un polynôme séparable. Alors l'homomorphisme*

$$r_{\mathfrak{P}} : G_{\mathfrak{P}} \to \mathrm{Gal}(B/\mathfrak{P}, A/\mathfrak{p})$$

est un isomorphisme.

Démonstration. Soient $\overline{A} = A/\mathfrak{p}$, $\overline{B} = B/\mathfrak{P}$. Le noyau de $r_{\mathfrak{P}}$ s'appelle le *sous-groupe d'inertie de $\mathfrak{P}$ et se note* $\mathfrak{I}_{\mathfrak{P}}$. Posons $f(X) = \prod_{1\leq i\leq d}(X - x_i)$ dans B, avec $x = x_1$; on a $\overline{f}(X) = \prod_{1\leq i\leq d}(X - \overline{x_i})$ dans $\overline{B}$. Soit $\sigma \in \mathfrak{I}_{\mathfrak{P}}$. On a donc $\overline{\sigma(x_i)} = \overline{x_i}$ pour tout $i = 1, \cdots, d$. Par suite $\overline{\sigma(x_1)} = \overline{x_1} \neq \overline{x_i}$ pour tout $i = 2, \cdots, d$. Il suit que $\sigma(x_1) = x_1$, c'est à dire que $\sigma =$id. □

Dans le résultat qui suit, K est toujours une extension finie de $\mathbb{Q}$ (resp. $\mathbb{F}_q(T)$) et A la fermeture intégrale de $\mathbb{Z}$ (resp. $\mathbb{F}_q[T]$) dans K.

Corollaire 7.4.7. *Soient $f \in A[X]$ un polynôme unitaire et irréductible, $\mathfrak{p}$ un idéal maximal de A. On pose $\overline{A} = A/\mathfrak{p}$ et l'on désigne par $\overline{f}$ le polynôme de $\overline{A}[X]$ obtenu en réduisant les coefficients de f modulo $\mathfrak{p}$. Soient E un corps de décomposition de f sur K, D la fermeture intégrale de A dans E et $\mathfrak{P}$ un idéal premier de D au dessus de $\mathfrak{p}$. On pose aussi $\overline{D} = D/\mathfrak{P}$. On suppose que $\overline{f}$ est un polynôme séparable.*

(i) Alors $\overline{D}$ est un corps de décomposition de $\overline{f}$ sur $\overline{A}$, E est galoisien sur K et le groupe de décomposition $G_{\mathfrak{P}}$ de $\mathfrak{P}$ est isomorphe par $r_{\mathfrak{P}}$ à $\mathrm{Gal}(\overline{D}, \overline{A})$.

(ii) Ecrivons $\overline{f}(X) = g_1 \cdots g_s$, avec $g_1, \cdots, g_s$ dans $\overline{A}[X]$ et irréductibles. Pour $1 \leq i \leq s$ soit Z_i l'ensemble des racines de f dans D qui modulo $\mathfrak{P}$ donnent les racines de g_i. Alors, pour tout $\sigma \in G_{\mathfrak{P}}$ et pour toute racine $x \in Z_i$ $(1 \leq i \leq s)$, on a $\sigma(x) \in Z_i$.

(iii) En particulier, si $\overline{f}(X) = g\prod_{1\leq i\leq r}(X - \overline{x_i})$, où $x_1, \cdots, x_r$ sont les racines de f (dans D) qui modulo $\mathfrak{P}$ sont dans $\overline{A}$ et où $g \in \overline{A}[X]$ est irréductible, alors $G_{\mathfrak{P}}$ est un groupe cyclique d'ordre $deg(f) - r$, engendré par un élément σ qui agit trivialement sur $\{x_1, \cdots, x_r\}$ et qui est un cycle d'ordre $deg(f) - r$ sur l'ensemble $\{x_{r+1}, \cdots, x_{deg(f)}\}$ des autres racines de f.

Démonstration. Comme $\overline{f}$ n'a que des racines simples, il en est de même de f et l'extension E/K est galoisienne. Ecrivons $f(X) = \prod_{1\leq i\leq d}(X - x_i)$, $x_i \in D$. Dans $\overline{D}$ on a $\overline{f}(X) = \prod_{1\leq i\leq d}(X - \overline{x_i})$ et les $\overline{x_i}$ sont deux à deux distincts. Considérons

$$\overline{A} \subseteq \overline{A}(\overline{x_1}, \cdots, \overline{x_d}) \subseteq \overline{D}.$$

On sait que $G_{\mathfrak{P}}$ se surjecte sur $\mathrm{Gal}(\overline{D},\overline{A})$, on voit, comme dans le corollaire précédent, que $G_{\mathfrak{P}}$ s'injecte dans $\mathrm{Gal}(\overline{A}(\overline{x_1},\cdots,\overline{x_d})/\overline{A})$. Donc $\overline{D} = \overline{A}(\overline{x_1},\cdots,\overline{x_d})$ et $G_{\mathfrak{P}} \simeq \mathrm{Gal}(\overline{D},\overline{A})$.

La partie (ii) résulte aussi du fait que, étant donné $\sigma \in G_{\mathfrak{P}}$, on a $\overline{\sigma(x)} = \overline{\sigma}(\overline{x})$ pour tout x appartenant à $\overline{D}$, donc

$$\overline{\sigma}(\overline{x_j}) = \overline{x_{j'}} \quad \Rightarrow \quad \sigma(x_j) = x_{j'} \ .$$

□

Exercice 7.1. (*S. Lang*) Soit L un corps de décomposition sur $\mathbb{Q}$ du polynôme

$$f(X) = X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15.$$

Montrer que le groupe de Galois de $L/\mathbb{Q}$ est isomorphe au groupe des permutations S_6.
(On pourra réduire modulo 2, 3, 5 et chaque fois utiliser 7.4.7.)

7.5 Exercices

Exercice 7.2. Soient A un anneau intègre, M un A-module. On note $T(M) := \{x \in M | \exists a \in A, a \neq 0, ax = 0\}$ l'ensemble des éléments de torsion de M. Montrer que $T(M)$ est un sous-A-module de M et que $M/T(M)$ est un A-module sans torsion. L'hypothèse "intègre" est-elle nécessaire ?

Exercice 7.3. 1) Montrer que toute famille libre du $\mathbb{Z}$-module $\mathbb{Q}$ est constituée d'un seul élément. Montrer que le $\mathbb{Z}$-module $\mathbb{Q}$ n'admet pas de base.

2) Soit $m \in \mathbb{Z}, m \geq 2$. Monter que le $\mathbb{Z}$-module $\mathbb{Z}/m\mathbb{Z}$ n'admet pas de famille libre.

3) Soit A un corps, alors un A-module M est noethérien si et seulement s'il est de dimension finie sur A.

4) Montrer que le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas noethérien.

5) Montrer que le $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ n'est pas noethérien.

6) Soit A un anneau. Montrer que $A[X]$ noethérien implique A noethérien.

7) Trouver deux anneaux A et B avec $A \subset B$, B noethérien et A non noethérien.

Exercice 7.4. Soient M un A-module noethérien, $u : M \to M$ une application A-linéaire surjective. Alors u est injective (considérer la suite $\ker(u^n)$).

Exercice 7.5. Soit $d \in \mathbb{Z}$, d non divisible par un carré, et $K = \mathbb{Q}(\sqrt{d})$.

1) Soit $x \in K$.

a) Justifier $x = a + b\sqrt{d}$ avec $a, b \in \mathbb{Q}$.

b) Montrer que x est entier sur $\mathbb{Z}$ si et seulement si $2a \in \mathbb{Z}$ et $a^2 - b^2 d \in \mathbb{Z}$.

c) Montrer que si x est entier sur $\mathbb{Z}$, alors $2b \in \mathbb{Z}$.

2) Montrer que la fermeture intégrale de $\mathbb{Z}$ dans K est : $\{\frac{a+b\sqrt{d}}{2} | a, b \in \mathbb{Z}, a \text{ et } b \text{ de même parité}\}$ si $d \equiv 1$ (modulo 4), et $\{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ si $d \not\equiv 1$ (modulo 4).

3) Déduire de ce qui précède que $\mathbb{Z}[\sqrt{5}]$ n'est pas intégralement clos.

Exercice 7.6. Soient p un nombre premier, ξ une racine primitive p-ième de l'unité dans $\mathbb{C}$, et $K = \mathbb{Q}(\xi)$.

1) Montrer que , pour tout $k = 1, \ldots, p-1$, $\mathrm{Tr}_{K/\mathbb{Q}}(\xi^k) = -1$ et $\mathrm{Tr}_{K/\mathbb{Q}}(1 - \xi^k) = p$.

2) Montrer que $\mathrm{N}_{K/\mathbb{Q}}(\xi - 1) = (-1)^{p-1} p$. En déduire que $p = (1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1})$.

3) On note A l'anneau des entiers de $\mathbb{Q}(\xi)$. Montrer que $A(1-\xi) \cap \mathbb{Z} = p\mathbb{Z}$.

4) Montrer que $\forall y \in A$, $\mathrm{Tr}_{K/\mathbb{Q}}(y(1-\xi)) \in p\mathbb{Z}$.

5) Déduire de ce qui précède que $A = \mathbb{Z}[\xi]$.

Exercice 7.7. Soit L un corps de décomposition sur $\mathbb{Q}$ de $P(X) = X^4 + 2X^2 + X + 3$.

1) a) Montrer que la réduction de P modulo 2 est un polynôme de degré 4 irréductible dans $\mathbb{F}_2[X]$.

b) En déduire que P est irréductible sur $\mathbb{Q}$. On peut donc identifier comme d'habitude $\mathrm{Gal}(L/\mathbb{Q})$ à un sous-groupe de S_4.

c) Montrer que $\mathrm{Gal}(L/\mathbb{Q})$ contient un cycle σ d'ordre 4.

2) a) On note $\overline{P}$ la réduction de P modulo 3. Décomposer $\overline{P}$ en produit de polynômes irréductibles dans $\mathbb{F}_3[X]$.

b) Montrer que $\mathrm{Gal}(L/\mathbb{Q})$ contient un cycle τ d'ordre 3.

3) a) On note $\widetilde{P}$ la réduction de P modulo 5. Décomposer $\widetilde{P}$ en produit de polynômes irréductibles dans $\mathbb{F}_5[X]$.

b) Montrer que $\mathrm{Gal}(L/\mathbb{Q})$ contient une transposition γ.

4) Déduire de ce qui précède que $\mathrm{Gal}(L/\mathbb{Q}) \cong S_4$.

5) Pour $X^4 + 2X^2 - 59X - 27$?

Exercice 7.8. Utiliser la méthode de l'exercice précédent pour étudier le groupe de Galois sur $\mathbb{Q}$ du polynôme $P(X) = X^6 + 18X^5 + 12X^4 - 6X^3 + 32X^2 + 13X + 45$.

Chapitre 8

Appendice : Les anneaux factoriels

Tous les anneaux sont supposés **commutatifs et unitaires.**

8.1 Généralités

Définition 8.1.1. Soit a un élément d'un anneau A. Soit b un élément de A, on dit que a divise b s'il existe un élément c de A tel que $a = bc$. On dit que a est irréductible dans A si a est non nul, non inversible et si pour tous b et c dans A

$$(a = bc) \Rightarrow (b \in A^* \text{ ou } c \in A^*).$$

Exemple 8.1.2. Dans $\mathbb{Z}$, les éléments irréductibles sont les $\pm p$, où p est un nombre premier.

Proposition 8.1.3. *Soient A un anneau intègre et a un élément de A. Alors, si l'idéal aA est premier, a est un élément irréductible de A.*

Démonstration. Ecrivons $a = bc$, avec b et c dans A. Puisque aA est premier, on a par exemple $b \in aA$, donc $b = ad$ avec $d \in A$. Il vient $a = bc = adc$, donc $1 = dc$ puisque A est intègre. □

La réciproque de cette proposition est fausse en général, la recherche de son champ de validité a, pour l'essentiel, conduit à la notion d'anneau factoriel. l'exercice suivant donne un exemple d'idéal non premier engendré par un irréductible.

Exercice 8.1. Soit $A = \mathbb{Z}[i\sqrt{3}] = \{a + bi\sqrt{3} \ / \ a, b \in \mathbb{Z}\}$ le sous-anneau de $\mathbb{C}$ engendré par $\mathbb{Z}$ et $i\sqrt{3}$. Montrer que 2, $1+i\sqrt{3}$ et $1-i\sqrt{3}$ sont des irréductibles de A mais que l'idéal $2A$ n'est pas premier (on a $(1 + i\sqrt{3})(1 - i\sqrt{3}) = 4$).

Définition 8.1.4. Soit A un anneau. On dit qu'un élément a de A, $a \neq 0$ et a non inversible, admet une factorisation unique en un produit d'irréductibles s'il existe $u \in A^*$, $p_1, \cdots, p_r \in A$ irréductibles tels que $a = up_1 \cdots p_r$ et tel que de plus, si $a = vq_1 \cdots q_s$ est une autre écriture semblable (avec donc v inversible et $q_1 \cdots q_s$ irréductibles), alors $r = s$, il existe $\varepsilon_1, \cdots, \varepsilon_r \in A^*$, il existe $\sigma \in \Sigma_r$ (Σ_r est le groupe des permutations de $\{1, \cdots, r\}$) vérifiant $p_i = \varepsilon_i q_{\sigma(i)}$, $1 \leq i \leq r$.

Remarque 8.1.5. Quelquefois on étend cette définition au cas où a est inversible en prenant alors $r = 0$, c'est à dire que le produit d'irréductibles apparaissant dans la factorisation de a est indexé sur l'ensemble vide, donc égal à 1.

Définition 8.1.6. On appelle anneau factoriel un anneau (commutatif, unitaire et) intègre dans lequel tout élément non inversible et non nul admet une factorisation unique en un produit d'irréductibles.

On sait que $\mathbb{Z}$ est factoriel. De même, $K[X]$ est factoriel, lorsque K est un corps (commutatif), ses irréductibles sont les polynômes irréductibles. On va montrer plus loin que tout anneau principal est factoriel et donner des exemples d'anneaux factoriels non principaux. La propriété pour un anneau d'être factoriel est assez forte, on rencontre facilement des anneaux qui ne le sont pas, comme par exemple $\mathbb{Z}[i\sqrt{3}]$ (cf 8.1, on a $(1 + i\sqrt{3})(1 - i\sqrt{3}) = 2 \times 2 = 4$).

Proposition 8.1.7. *Soient A un anneau factoriel et a un élément non nul de A. Alors l'idéal aA est premier si et seulement si a est irréductible.*

Démonstration. Soit a un élément irréductible de A et soient b, c des éléments de A tels que $bc \in aA$. Il existe donc un élément d de A tel que $bc = ad$. On écrit alors les factorisations de b, c et d en produits d'irréductibles, à cause de l'unicité a figure à facteur inversible près dans celle de b ou celle de c, donc b ou c est dans aA. La réciproque est donnée par 8.1.3. □

Cette proposition "caractérise presque" les anneaux factoriels, comme le montre le théorème suivant.

Théorème 8.1.8. *Soit A un anneau (commutatif, unitaire,) intègre et noethérien. Alors les assertions suivantes sont équivalentes :*
(i) A est factoriel,
(ii) pour tout élément irréductible q de A, l'idéal qA est premier.

Démonstration. Il faut prouver que (ii) implique (i).

Lemme 8.1.9. *Soit A un anneau intègre et noethérien. Alors tout élément de A s'écrit sous la forme d'un produit fini d'éléments irréductibles.*

Preuve du lemme. Soit $\mathcal{I}$ l'ensemble des idéaux de A de la forme aA, où $a \neq 0$, $a \notin A^*$ et a n'est pas égal à un produit fini d'éléments irréductibles de A. Supposons $\mathcal{I} \neq \emptyset$, alors $\mathcal{I}$ possède un élément maximal aA (c'est ici qu'intervient l'hypothèse "noethérien"). Par définition de $\mathcal{I}$ a n'est pas irréductible, c'est à dire qu'il existe b et c dans A tels que $a = bc$, $b \notin A^*$, $c \notin A^*$. On voit alors que bA contient aA et $bA \neq aA$ (c'est pour cette dernière relation que l'on utilise le fait que A est intègre) ; de même cA contient aA et $cA \neq aA$. Ainsi, bA et cA ne sont pas dans $\mathcal{I}$, par suite b et c sont égaux à des produits finis d'irréductibles, également $a = bc$, ce qui est une contradiction. Donc $\mathcal{I}$ est vide. □

Suite de la démonstration de 8.1.8. Il faut prouver l'unicité. Soit

$$up_1 \cdots p_r \;=\; vq_1 \cdots q_s$$

avec $u, v \in A^*$, $p_1, \cdots, p_r, q_1, \cdots, q_s$ irréductibles et par exemple $r \leq s$. Alors $up_1 \cdots p_r$ est dans $q_1 A$, donc, puisque ce dernier est un idéal premier, il existe i tel que $p_i \in q_1 A$, par suite, puisque p_i est irréductible, $p_i = \varepsilon_1 q_1$ avec $\varepsilon_1 \in A^*$. Après simplification il vient

$$(u\varepsilon_1)p_1 \cdots p_{i-1}p_{i+1} \cdots p_r \;=\; vq_2 \cdots q_s.$$

La première relation comporte r irréductibles à gauche et s à droite, dans la deuxième ces nombres sont devenus $r-1$ et $s-1$.

On recommence ..., il vient une relation de la forme $u' = vq_{r+1} \cdots q_s$, où $u' \in A^*$, qui n'est possible que si $r = s$. □

Proposition 8.1.10. *Soient A un anneau factoriel et $\mathfrak{P}$ un idéal premier de A minimal (pour l'inclusion) parmi les idéaux premiers non nuls de A. Alors $\mathfrak{P}$ est principal.*

Démonstration. Soit $a \in \mathfrak{P}$, $a \neq 0$. Soit $a = up_1 \cdots p_r$ l'écriture de a en produit d'irréductibles. On voit qu'il existe i tel que $p_i \in \mathfrak{P}$. Alors $p_i A$ est un idéal premier (car A est factoriel) non nul contenu dans $\mathfrak{P}$, donc $p_i A = \mathfrak{P}$. □

Exercice 8.2. Montrer la réciproque de la proposition 8.1.10.

Définition 8.1.11. Soit A un anneau factoriel. Soient a et b deux éléments non nuls de A. On pose

$$a = up_1^{n_1} \cdots p_r^{n_r} \quad , \quad b = vp_1^{m_1} \cdots p_r^{m_r},$$

où $u, v \in A^*$, $p_1, \cdots, p_r$ sont irréductibles, $p_i \notin A^* p_j$ si $i \neq j$, et où les n_i et les m_j sont des entiers naturels.

Un plus grand diviseur de a et b est

$$\mathrm{pgcd}(a, b) = p_1^{\min(n_1, m_1)} \cdots p_r^{\min(n_r, m_r)},$$

il est défini à facteur inversible près.

Un plus petit commun multiple de a et b est

$$\text{ppcm}(a,b) = p_1^{\max(n_1,m_1)} \cdots p_r^{\max(n_r,m_r)},$$

il est défini à facteur inversible près.

On peut remarquer que les *idéaux* $\text{pgcd}(a,b)A$ et $\text{ppcm}(a,b)A$ sont bien définis.

Exercice 8.3. Justifier les expressions "*plus grand* diviseur" et "*plus petit* commun multiple" ; de quel ordre et sur quel ensemble s'agit-il ? (Montrer que $\text{pgcd}(a,b)$ est multiple de tout diviseur commun à a et b, de même que $\text{ppcm}(a,b)$ divise tout multiple commun à a et b.)

Exercice 8.4. Soient A un anneau factoriel, a, b et c des éléments non nuls de A. On suppose que a divise le produit bc et que a et b sont premiers entre eux (i.e. leurs pgcd sont inversibles), montrer qu'alors a divise c (ceci s'appelle parfois le lemme de Gauss).

8.2 Anneaux principaux et anneaux factoriels

Théorème 8.2.1. *Soit A un anneau principal, alors A est factoriel.*

Démonstration. Soit p un irréductible de A, montrons que l'idéal pA est premier. Il existe un idéal maximal $\mathfrak{M}$ qui contient pA et il existe $q \in A$ tel que $\mathfrak{M} = qA$. On a $pA \subset qA$, il suit par les raisonnements habituels et par ce que p est irréductible que $pA = qA$. Donc pA est maximal, par suite premier.

L'anneau est principal, donc noethérien ; la conclusion vient donc de 8.1.8. □

Proposition 8.2.2. *Soient A un anneau principal, a et b deux éléments non nuls de A, alors*

$$aA \cap bA = ppcm(a,b)A \quad , \quad aA + bA = pgcd(a,b)A.$$

En particulier (formule de Bézout) il existe deux éléments u et v de A tels que

$$ua + vb = pgcd(a,b).$$

Démonstration. Il existe $c \in A$ tel que $aA \cap bA = cA$, d'autre part, comme a et b divisent $\text{ppcm}(a,b)$, il vient $\text{ppcm}(a,b)A \subset aA \cap bA$, d'où l'égalité cherchée. L'autre relation se montre de même. □

Théorème 8.2.3. *Soit A un anneau factoriel. On suppose que dans A la formule de Bézout est vraie, c'est à dire que quel que soient les éléments non nuls a et b de A, il existe u et v dans A tels que $ua + vb = pgcd(a,b)$. Alors A est un anneau principal.*

Démonstration. Soit I un idéal de A, $I \neq (0)$. Soit $x_1 \in I$, $x_1 \neq 0$. Si $I \neq x_1 A$, alors il existe $x_2' \in I - x_1 A$. Soit $x_2 = \mathrm{pgcd}(x_1, x_2')$. Avec la formule de Bézout on voit alors que $x_1 A + x_2' A = x_2 A$. On recommence avec x_2 à la place de x_1, etc. Si I n'est pas principal, on fabrique ainsi une suite strictement croissante d'idéaux de A

$$x_1 A \subset x_2 A \subset x_3 A \subset \cdots$$

donc une suite infinie $x_1, x_2, x_3, \cdots$ où x_2 est un diviseur strict de x_1, où x_3 est un diviseur strict de x_2, etc. Ceci est impossible car le nombre de diviseurs (à facteurs inversibles près) de x_1 est fini. □

Exercice 8.5. Soient A un anneau factoriel et a un élément de A. On pose $a = u p_1^{n_1} \cdots p_r^{n_r}$ où $u \in A^*$, $p_1, \cdots, p_r$ sont irréductibles, $p_i \notin A^* p_j$ si $i \neq j$, et où les n_i sont des entiers naturels. Montrer que le nombre de diviseurs (à facteurs inversibles près) de a est

$$\prod_{1 \leq i \leq r} (n_i + 1).$$

8.3 Anneaux factoriels et polynômes

Lemme 8.3.1. *Soient A un anneau et $\mathfrak{P}$ l'un de ses idéaux premiers. Soit $\mathfrak{P}A[X]$ l'idéal de l'anneau des polynômes $A[X]$ engendré par $\mathfrak{P}$ (donc l'idéal des éléments de $A[X]$ à coefficients dans $\mathfrak{P}$). Alors $\mathfrak{P}A[X]$ est un idéal premier de $A[X]$.*

Démonstration. Soit $s : A \to A/\mathfrak{P}$ la surjection canonique et soit

$$\varphi : A[X] \to (A/\mathfrak{P})[X]$$

l'homomorphisme qui au polynôme $\sum a_i X^i$ associe $\sum s(a_i) X^i$. Il est clair que φ est surjectif, son noyau est l'ensemble des éléments $\sum a_i X^i$ de $A[X]$ tels que $\sum s(a_i) X^i = 0$ dans $(A/\mathfrak{P})[X]$, c'est donc $\mathfrak{P}A[X]$. Le théorème de factorisation montre alors que l'on a un isomorphisme

$$\overline{\varphi} : A[X]/\mathfrak{P}A[X] \simeq A/(\mathfrak{P})[X]$$

et le membre de droite est un anneau intègre. □

Remarque 8.3.2. L' isomorphisme

$$\overline{\varphi} : A[X]/\mathfrak{P}A[X] \simeq A/(\mathfrak{P})[X],$$

qui est canonique, est en soi intéressant. Il vérifie

$$\overline{\varphi} \circ t = \varphi,$$

où $t : A[X] \to A[X]/\mathfrak{P}A[X]$ est la surjection canonique.

Corollaire 8.3.3. *Soient A un anneau factoriel, p un élément irréductible de A. Alors l'idéal $pA[X]$, des éléments de $A[X]$ dont tous les coefficients sont divisibles par p, est premier.*

Corollaire 8.3.4. *Soient A un anneau factoriel, K son corps des fractions et $P \in A[X]$. On suppose que $P = FG$ dans $K[X]$ (c'est à dire que F et G sont dans $K[X]$), alors il existe $\lambda \in K^*$ tel que λF et $\lambda^{-1}G$ soient dans $A[X]$ (donc $P = (\lambda F)(\lambda^{-1}G)$ dans $A[X]$).*

Démonstration. Soit d un dénominateur commun à tous les coefficients de F et G. Posons $F_1 = dF$ et $G_1 = dG$, ce sont des éléments de $A[X]$ et l'on a

$$d^2P = F_1G_1.$$

Soit p un diviseur irréductible de d^2, alors, d'après (3.2), p divise tous les coefficients de F_1 ou de G_1, par exemple ceux de F_1. On pose $pF_2 = F_1$, $G_2 = G_1$ et $D_2 = pd^2$, avec donc F_2 et G_2 dans $A[X]$, D_2 dans A. Les polynômes F_2 et G_2 sont des multiples par des éléments de K^* de F et G respectivement et l'on a

$$D_2P = F_2G_2.$$

On recommence avec un diviseur irréductible de D_2, etc. Finalement, au bout d'un nombre fini d'étapes, on voit qu'il existe λ et μ dans K^* tels que

$$P = (\lambda F)(\mu G)\ ,\ (\lambda F) \in A[X]\ ,\ (\mu G) \in A[X].$$

On a $\lambda\mu = 1$ car $P = FG$. □

Remarque 8.3.5. Ce corollaire est faux si A n'est pas factoriel, comme le montre l'exemple suivant : $A = \mathbb{Z}[i\sqrt{3}]$, donc $K = \mathbb{Q}(i\sqrt{3})$ et

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

Définition 8.3.6. Soient A un anneau factoriel. Un élément de $A[X]$ est dit primitif si les pgcd de ses coefficients sont inversibles.

Théorème 8.3.7. *Soit A un anneau factoriel. Alors l'anneau des polynômes $A[X]$ est factoriel. On a $A[X]^* = A^*$, les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A et les polynômes de $A[X]$ irréductibles dans $K[X]$ (K est le corps des fractions de A) et primitifs.*

Démonstration. On sait que $A[X]^* = A^*$. Soit $P \in A[X]$, non nul et non inversible. On écrit $P = P_1 \cdots P_r$, sa décomposition en produit d'irréductibles dans $K[X]$ (ce dernier est factoriel car principal). Un peu d'arithmétique montre alors qu'il existe deux éléments a et b de A, non nuls, tels que

$$aP = bQ_1 \cdots Q_r$$

avec, pour $1 \leq i \leq r$, Q_i dans $A[X]$, primitif, égal à P_i à un facteur de K^* près. Soit p un diviseur irréductible de a, alors, cf (3.2), p divise b ou tous les coefficients de l'un des Q_i, ces derniers étant primitifs, on a que p divise b. On recommence ..., il vient que a divise b.

On a donc prouvé l'existence de la décomposition suivant un produit d'irréductibles de A et de polynômes de $A[X]$ irréductibles dans $K[X]$ et primitifs. L'unicité de cette écriture découle facilement de celles dans A et $K[X]$. Il en résulte que la famille des irréductibles de $A[X]$ est bien celle annoncée, comme le montre l'exercice 8.6 suivant. □

Corollaire 8.3.8. *Soit A un anneau factoriel, alors $A[X_1, \cdots, X_n]$ est factoriel.*

Exercice 8.6. Soient A un anneau et $\mathcal{P}$ une famille d'éléments non nuls et non inversibles de A possédant la propriété suivante : tout élément a non nul et non inversible de A s'écrit sous la forme $a = \epsilon p_1 \cdots p_r$ avec $\epsilon \in A^*$ et $p_1 \cdots p_r$ dans $\mathcal{P}$, de plus cette écriture est unique - au sens de la définition (1.4). Alors A est factoriel et ses irréductibles sont, à facteurs inversibles près, les éléments de $\mathcal{P}$.

Exercice 8.7. Montrer que $A[X]$ est principal si et seulement si A est un corps.

Exercice 8.8. Montrer que dans $\mathbb{Z}[X]$, $X^2 + 2$ et $X + 2$ sont premiers entre eux et ne vérifient pas la formule de Bézout.

Exercice 8.9. Soient A un anneau et $(X_n)_{n\in\mathbb{N}}$ des indéterminées. On a de manière évidente

$$A[X_1, \cdots, X_n] \subset A[X_1, \cdots, X_m]$$

si $n \leq m$, donc on peut former l'anneau

$$B = \cup_{n\in\mathbb{N}} A[X_1, \cdots, X_n].$$

On suppose que A est factoriel, montrer qu'il en est alors de même de B. Montrer que B n'est pas noethérien.

Théorème 8.3.9. *(Critère d'Eisenstein) Soient A un anneau factoriel, K le corps des fractions de A et*

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n \in A[X]$$

avec $degf(X) = n \geq 1$. On suppose qu'il existe un élément irréductible p de A tel que :
p ne divise pas a_n,
p divise tous les a_i pour $0 \leq i \leq n-1$,
p^2 ne divise pas le terme constant a_0.

Alors $f(X)$ est irréductible dans $K[X]$. Si de plus $f(X)$ est primitif, alors il est irréductible dans $A[X]$.

Démonstration. Soit $s : A \to A/pA$ la surjection canonique et

$$\varphi : A[X] \to \frac{A}{pA}[X]$$

l'homomorphisme qui à $P = \sum a_i X^i$ associe $P^s := \sum s(a_i)X^i$.

Ecrivons $f = PQ$ dans $K[X]$. Grâce à 8.3.4 on peut supposer que P et Q sont dans $A[X]$. Posons

$$P = \sum_{0 \leq i \leq u} b_i X^i \ , \ Q = \sum_{0 \leq i \leq v} c_i X^i$$

avec donc les b_i et c_i dans A ; on suppose de plus que l'on a une vraie factorisation de f, c'est à dire que $\deg P = u \geq 1$ et $\deg Q = v \geq 1$. Appliquant φ à l'égalité $f = PQ$, il vient compte tenu des hypothèses

$$s(a_n)X^n = f^s = P^s Q^s.$$

Comme l'anneau A/pA est intègre, on voit que les diviseurs de $s(a_n)X^n$ sont de la forme αX^m avec $\alpha \in A/pA$ et $m \leq n$, il suit que $P^s = \alpha X^{u'}$ et $Q^s = \beta X^{v'}$ avec α et β dans A/pA, $u' + v' = n$. Comme $u' \leq u$ et $v' \leq v$ il vient $u' = u$ et $v' = v$. Donc P^s et Q^s sont tous deux de degrés plus grands que 1, leurs termes constants sont nuls. On a donc $s(b_0) = 0$ et $s(c_0) = 0$, par suite p divise b_0 et c_0 d'où p^2 divise $a_0 = b_0 c_0$ (on utilise ici le fait que A est factoriel), ce qui contredit une hypothèse. La factorisation $f = PQ$ n'existe donc pas. □

Exercice 8.10. Montrer que $2X^7 + 6X^4 + 18X + 12$ est irréductible dans $\mathbb{Q}[X]$. Donner la décomposition de ce polynôme en produit d'irréductibles dans $\mathbb{Z}[X]$.

Exercice 8.11. Soient K un corps et $f(T) \in K[T]$ possédant une racine simple dans une extension de K. Soit $n > 0$ un entier. Montrer que $X^n - f(T)$ est irréductible dans $K[X, T]$.

8.4 Anneaux factoriels et anneaux de fractions

Soit A un anneau. Une partie S de A est dite *multiplicativement fermée* si

$$1 \in S \ , \ 0 \notin S \ , \ (x, y \in S \Rightarrow xy \in S).$$

Soit donc S une partie multiplicativement fermée d'un anneau A *intègre* de corps des fractions K et soit

$$S^{-1}A := \{\frac{a}{s} \ / \ a \in A \ , \ s \in S\}.$$

C'est un sous-anneau de K ; $(S^{-1}A)^*$ est l'ensemble des a/s (avec donc $a \in A$, $s \in S$) tels que a divise un élément de S ; les idéaux premiers de $S^{-1}A$ sont de la forme $\mathfrak{p}S^{-1}A$ où $\mathfrak{p}$ est un idéal premier de A *ne rencontrant pas* S (ceci donne en fait une bijection croissante entre les idéaux premiers de A ne rencontrant pas S et ceux de $S^{-1}A$).

Théorème 8.4.1. *Soient A un anneau factoriel et S une partie multiplicativement fermée de A. Alors l'anneau $S^{-1}A$ est factoriel. Les éléments irréductibles de $S^{-1}A$ sont, à un facteur multiplicatif de $S^{-1}A^*$ près, les irréductibles de A qui ne divisent aucun élément de S.*

Une fois énoncée la famille d'irréductibles de $S^{-1}A$, la démonstration de ce théorème est très simple et laissée au lecteur.

Exercice 8.12. Soient K un corps et $K[X, 1/X]$ le sous-anneau de $K(X)$ engendré par K, X et $1/X$. Montrer que $K[X, 1/X]$ est factoriel.

Exercice 8.13. Etant donné un anneau A et $\mathfrak{p}$ l'un de ses idéaux premiers, on note $A_{\mathfrak{p}}$ l'anneau $S^{-1}A$ pour $S = A - \mathfrak{p}$, c'est un anneau local (cela veut dire qu'il ne possède qu'un seul idéal maximal) d'idéal maximal $\mathfrak{p}A_{\mathfrak{p}}$. Soit A un anneau factoriel et p l'un de ses éléments irréductibles. Montrer que A_{pA} est un anneau factoriel ne possédant qu'un seul irréductible (à facteurs inversibles près), qui est p. En déduire que les idéaux de A_{pA} sont de la forme $p^n A_{pA}$, où $n \geq 0$ est un entier.

8.5 Exercices

Exercice 8.14. 1) Soient A un anneau factoriel, K son corps des fractions, $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ et $0 \neq r = \frac{b}{c} \in K$, $(b,c) = 1$. Si r est une racine de $P(X)$ dans K (i.e. $P(r) = 0$), alors $b \mid a_0$ et $c \mid a_n$.

2) Trouver toutes les racines dans $\mathbb{Q}$ du polynôme $2X^4 - X^3 - X^2 - X - 3 \in \mathbb{Z}[X]$.

Exercice 8.15. Soient A un anneau factoriel, $\mathfrak{p}$ un idéal premier de A et $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$. On note $\overline{P}(X) = \overline{a_n}X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_0} \in (A/\mathfrak{p})[X]$ induit par la surjection canonique $A \to A/\mathfrak{p}, a \mapsto \overline{a}$.

1) Supposons que $a_n = 1$, montrer que $\overline{P}(X)$ irréductible $\Rightarrow P(X)$ irréductible.

2) Donner un exemple avec $a_n \neq 1$, $\overline{P}(X)$ irréductible, mais $P(X)$ réductible.

3) Utiliser 1) avec $\mathbb{Z}/2\mathbb{Z}$ pour montrer que $P(X) = X^6 + 18X^5 + 12X^4 - 6X^3 + 32X^2 + 13X + 45$ est irréductible dans $\mathbb{Z}[X]$.

Exercice 8.16. 1) Montrer qu'un anneau principal est factoriel et que tout idéal premier non nul est maximal.

2) Inversement, soit A un anneau factoriel dans lequel tout idéal premier non nul est maximal. On va montrer que A est principal.

2-i) Montrer que tout idéal premier est principal.

2-ii) Soit $I = (a,b)$ un idéal et d un plus grand commun diviseur de a et b. On note $a = a'd$, $b = b'd$. Montrer que $(a',b') = A$, en déduire que $I = (d)$, i.e. la formule de Bézout est vraie dans A. En déduire que A est principal.

Exercice 8.17. Soient $K \subset L$ deux corps, $P, Q \in K[X] \setminus \{0\}$, D un pgcd de P et Q dans $K[X]$. Montrer que D est aussi un pgcd de P et Q dans $L[X]$.

Exercice 8.18. Soit A un anneau commutatif unitaire et intègre. On dit que A est un anneau **euclidien** s'il existe une application $\varphi : A \setminus \{0\} \to \mathbb{N}$ telle que :

(i) $\forall a, b \in A \setminus \{0\}, \varphi(a) \leq \varphi(ab)$ ($\Leftrightarrow$ (i') $\forall x, y \in A, x|y \Rightarrow \varphi(x) \leq \varphi(y)$).

(ii) $\forall a, b \in A \setminus \{0\}, \exists q, r \in A$ tels que $a = bq + r$ et que $\varphi(r) < \varphi(b)$ si $r \neq 0$.

1) Montrer que si φ vérifie

$$\forall a, b \in A \setminus \{0\}, a \neq b \Rightarrow \varphi(a-b) \leq \max(\varphi(a), \varphi(b)),$$

alors $\forall a, b \in A \setminus \{0\}$, le couple (q,r) dans (ii) est unique.

2) Soit I un idéal de $A, I \neq (0)$.

a) Montrer qu'il existe $a \in I \setminus \{0\}$ tel que $\forall x \in I \setminus \{0\}$, $\varphi(a) \leq \varphi(x)$.

b) Montrer que $I = (a)$, en déduire que tout anneau euclidien est principal.

3) Soit $a \in A \setminus \{0\}$. Montrer que $\varphi(1_A) \leq \varphi(a)$ et que $a \in A^\times \Leftrightarrow \varphi(a) = \varphi(1_A)$.

4) Montrer que $\mathbb{Z}$ est euclidien.

5) Soit K un corps. Montrer que $K[X]$ est euclidien.

6) Soit $d \in \{-2, -1, 2, 3\}$. Montrer que $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ est un anneau euclidien. Calculer $\mathbb{Z}[i]^\times$.

Exercice 8.19. (**Algorithme d'Euclide**). Soit (A, φ) un anneau euclidien. Soit $a, b \in A \setminus \{0\}$. En utilisant de manière répétitive la condition ii) de la définition de l'anneau euclidien (cf. exercice 8.18), on a

$$\begin{aligned}
&a = q_0 b + r_1, r_1 = 0 \text{ ou } \varphi(r_1) < \varphi(b);\\
&b = q_1 r_1 + r_2, r_2 = 0 \text{ ou } \varphi(r_2) < \varphi(r_1);\\
&r_1 = q_2 r_2 + r_3, r_3 = 0 \text{ ou } \varphi(r_3) < \varphi(r_2);\\
&\vdots\\
&r_k = q_{k+1} r_{k+1} + r_{k+2}, r_{k+3} = 0 \text{ ou } \varphi(r_{k+2}) < \varphi(r_{k+1});
\end{aligned}$$

En notant $r_0 = b$ et n le plus petit entier ≥ 0 tel que $r_{n+1} = 0$ (Remarque : un tel n existe car $\{\varphi(r_k)\}_{k \in \mathbb{N}}$ est une suite d'entiers positifs et strictement décroissante), montrer que r_n est un pgcd de a et b.

Exercice 8.20. Soient K un corps, $a, b \in \mathbb{N}^*$, et $0 < d = \text{ pgcd}(a, b)$. Montrer que $X^d - 1 = \text{ pgcd}(X^a - 1, X^b - 1)$ dans $K[X]$.

Exercice 8.21. Soient p un nombre premier et $P(X) = X^{p-1} + X^{p-2} + \cdots + 1$. Montrer que $P(X)$ est irréductible dans $\mathbb{Z}[X]$. (Indication : $(X-1)P(X) = X^p - 1$.)

Exercice 8.22. Soient $P(X)$ un polynôme irréductible de $\mathbb{Z}[X]$ et $S = \{P(X)^n \mid n \in \mathbb{N}\}$.

1) Quels sont les éléments inversibles de $S^{-1}\mathbb{Z}[X]$?

2) Montrer que $S^{-1}\mathbb{Z}[X]$ est un anneau factoriel. Quels sont ses éléments irréductibles ?

Exercice 8.23. Soient $S = \{10^n | n \in \mathbb{N}\}$, $A = S^{-1}\mathbb{Z}$.

1) Montrer que $A^\times = \{\pm 2^a 5^b | a, b \in \mathbb{Z}\}$.

2) Montrer que les idéaux premiers de A sont de la forme pA où p est nul ou bien est un nombre premier différent de 2 et 5.

3) Montrer que A est factoriel. Quels sont ses élément irréductibles ?

Chapitre 9

Exercices complémentaires

Examen partiel du 22/11/99

I. Soient L/K une extension finie et ξ un élément de L tel que $L = K(\xi)$. Pour tout $\alpha \in L$, on désigne par f_α l'application de L dans lui même définie par $f_\alpha(x) = \alpha x$ (pour tout $x \in L$). C'est une application K-linéaire.

1) Montrer que $\det(X \cdot id - f_\xi) = \mathrm{irr}(\xi, K; X)$.

2) Pour quels α de L a-t-on $\det(X \cdot id - f_\alpha) = \mathrm{irr}(\alpha, K; X)$?

II. Soit $P(X) = X^3 + 2X + 2 \in \mathbb{Q}[X]$.

1) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$, que $P(X)$ admet une et une seule racine réelle.

On notera θ la racine réelle de $P(X)$, par θ_1 et θ_2 les deux autres racines de $P(X)$, dans $\mathbb{C}$.

2) a) Montrer que l'extension $\mathbb{Q}(\theta, \theta_1)/\mathbb{Q}$ est de degré 6.

b) Montrer que $\mathbb{Q}(\theta, \theta_1)$ est un corps de décomposition de $P(X)$ sur $\mathbb{Q}$.

c) Soit ω un nombre complexe tel que $\omega^2 = -(3\theta^2 + 8)$. Montrer que

$$\mathbb{Q}(\theta, \theta_1) = \mathbb{Q}(\theta, \omega)$$

(on pourra examiner le discriminant du polynôme minimal de θ_1 sur $\mathbb{Q}(\theta)$).

3) a) Soit j l'homomorphisme inclusion $j : \mathbb{Q}(\theta) \hookrightarrow \mathbb{C}$. Expliquer pourquoi j possède deux prolongements à $\mathbb{Q}(\theta, \omega)$, que l'on notera j_1 et j_2.

b) Soit σ_1 le $\mathbb{Q}$-homomorphisme de $\mathbb{Q}(\theta)$ dans $\mathbb{C}$ qui à θ associe θ_1. Décrire les prolongements de σ_1 à $\mathbb{Q}(\theta, \omega)$.

c) Soit

$$\mathfrak{I} = \{\tau(\omega) \ / \ \tau \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\theta, \omega), \mathbb{C})\}.$$

Montrer que le cardinal de $\mathfrak{I}$ est 6.

d). Montrer que $\mathbb{Q}(\omega)$ est un corps de décomposition de $P(X)$ sur $\mathbb{Q}$.

III. 1) Soit K un corps de caractéristique $p > 0$ et soit P un élément de $K[X]$ qui s'écrit $P(X) = Q(X^p)$, pour un certain élément Q de $K[X]$. Soit

$P = FG$ une factorisation de P dans $K[X]$, où F et G sont premiers entre eux.

a) Montrer que les polynômes dérivés F' et G' vérifient $F' = G' = 0$ (on pourra utiliser la formule $0 = (FG)'$).

b) En déduire que F et G sont eux aussi des polynômes en X^p.

Dorénavant, on pose $P(X) = X^{p^2} - X^p - \lambda$, *où* $\lambda \in K \setminus K^p$, $Q(X) = X^p - X - \lambda$. *On désigne par* $K^{alg.}$ *une clôture algébrique de* K.

2) a) Soit θ une racine de Q, dans $K^{\text{alg.}}$. Montrer que les racines de Q (dans $K^{\text{alg.}}$) sont les $\theta + u$ où $u \in K^{\text{alg.}}$ vérifie $u^p = u$.

b) On suppose que Q n'a pas de racine dans K, montrer qu'alors Q est irréductible sur K.

c) Toujours sous l'hypothèse que Q est sans racine dans K, montrer que P est irréductible sur K.

3) Dans cette question, on suppose que $K = \mathbb{F}(T)$, où $\mathbb{F}$ est un corps fini, et l'on choisit $\lambda = T$, donc $P(X) = X^{p^2} - X^p - T$ et $Q(X) = X^p - X - T$. Soit α une racine de P, dans $K^{\text{alg.}}$. Quel est le nombres de K-homomorphismes de $K(\alpha)$ dans $K^{\text{alg.}}$?

Examen du 07/02/00

I. Soit

$$P(X) = X^4 + X^2 - 5X + 13 \in \mathbb{Q}[X]$$

et soient L un corps de décomposition de $P(X)$ sur $\mathbb{Q}$, $G = \text{Gal}(L/\mathbb{Q})$. Soient θ_i, $1 \leq i \leq 4$, les racines de $P(X)$ dans L.

1) En réduisant $P(X)$ modulo 3, montrer que $P(X)$ est irréductible sur $\mathbb{Q}$.

2) En examinant $P(X)$ modulo 2, montrer que G possède un élément σ d'ordre 3, qui laisse fixe l'un des θ_i, que l'on notera θ_1.

3) Montrer qu'il existe un élément τ de G laissant fixe deux racines de $P(X)$ et échangeant les deux autres (on pourra réduire modulo 5).

4) Déduire des questions précédentes que G est isomorphe au groupe symétrique S_4.

II. Soit

$$P(X) = X^4 + X^3 + 5X^2 + X + 1 \in \mathbb{Q}[X].$$

On pourra remarquer que, dans $\mathbb{C}[X]$

$$P(X) = (X^2 + \frac{1 + i\sqrt{11}}{2}X + 1)(X^2 + \frac{1 - i\sqrt{11}}{2}X + 1).$$

Soient L le corps de décomposition, dans $\mathbb{C}$, de $P(X)$ et $\theta \in L$ une racine de $P(X)$. On pose $G = \text{Gal}(L/\mathbb{Q})$.

1) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$ et que G contient un élément d'ordre 4 (on pourra réduire modulo 2).

2) a) Montrer que l'extension $\mathbb{Q}(i\sqrt{11},\theta)/\mathbb{Q}$ est de degré 4.

b) On suppose que $\mathbb{Q}(i\sqrt{11},\theta) = L$, montrer qu'alors G contient deux éléments d'ordre 2.

c) En déduire que l'extension $L/\mathbb{Q}$ est de degré 8.

On désigne par $\theta_1 = \theta, \theta_2$ les racines dans $\mathbb{C}$ de $Q_1(X) = X^2 + \frac{1+i\sqrt{11}}{2}X + 1$, par θ_3, θ_4 celles de $Q_2(X) = X^2 + \frac{1-i\sqrt{11}}{2}X + 1$.

3) On pose $\mathrm{Gal}(\mathbb{Q}(i\sqrt{11})/\mathbb{Q}) = \{id, \sigma_1\}$.

a) Montrer que σ_1 admet un prolongement σ à L caractérisé par

$$\sigma(\theta_1) = \theta_3 \quad , \quad \sigma(\theta_3) = \theta_2.$$

b) Montrer que σ est d'ordre 4.

c) Montrer qu'il existe un élément τ de G tel que

$$\tau(i\sqrt{11}) = i\sqrt{11}\ ,\ \tau(\theta_1) = \theta_2\ ,\ \tau(\theta_2) = \theta_1\ ,\ \tau(\theta_3) = \theta_3\ ,\ \tau(\theta_4) = \theta_4.$$

d) Montrer que

$$G = \{\tau^i\sigma^j \ / \ i = 0,1 \text{ et } 0 \leq j \leq 3\}.$$

4) Montrer que $L = \mathbb{Q}(\theta_1 - \theta_3)$.

III. Soient $p > 2$ un nombre premier et $\mathbb{F}_p$ un corps à p éléments. Soient $K = \mathbb{F}_p(T)$ et

$$P(X) = X^{p^2} + (T^2 - 1)X^p + T + 1 \in K.$$

On désigne par L un corps de décomposition de $P(X)$ sur K et par $\theta \in L$ une racine de $P(X)$. Soit $G = \mathrm{Aut}_K(L)$.

1) a) Montrer que $P(X)$ est irréductible dans $K[X]$.

b) Dans une clôture algébrique de L soient u et v définis par

$$u^p = 1 - T^2 \quad , \quad v^{p-1} = u.$$

Montrer que les racines de P(X) sont les $\theta + tv$ où t décrit $\mathbb{F}_p$, que u et v sont dans L, que $L = K(\theta, v)$.

2) a) Montrer que l'extension $L/K(\theta^p, v)$ est de degré 1 ou p.

b) On suppose que $L = K(\theta^p, v)$, montrer qu'alors $\theta \in K(\theta^p, u)$ (on pourra remarquer que$K(\theta^p, v)$ est une extension séparable de $K(\theta^p, u)$).

c) Montrer que $\theta \notin K(\theta^p, u)$ (on pourra poser $\theta = \sum_{0 \leq i,j < p-1} \lambda_{i,j}\theta^{pi}u^j$ avec $\lambda_{i,j} \in K$ et élever à la puissance p...).

3) Quel est le degré de séparabilité de L sur K ? Montrer que

$$L^G = K(u, \theta^p - u\theta).$$

Examen de septembre 2000

I. Soit le polynôme

$$P(X) = 3X^5 - 12X^3 + 12X - 1 \in \mathbb{Q}[X].$$

1) Montrer que $P(X)$ est irréductible sur $\mathbb{Q}$ (on pourra "changer X en $1/X$").

2) Montrer que $P(X)$ possède trois racines réelles exactement (on pourra étudier sur $\mathbb{R}$ la fonction polynôme $x \mapsto P(x)$).

3) Soit L un un corps de décomposition de $P(X)$ sur $\mathbb{Q}$.

a) Déduire des questions précédentes que le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q})$ contient un élément d'ordre 2 et un élément d'ordre 5.

b) Montrer que $\mathrm{Gal}(L/K)$ est isomorphe à Σ_5, le groupe des permutations d'un ensemble à 5 éléments.

c) Montrer que l'équation $P(X) = 0$ n'est pas résoluble par radicaux sur le corps des rationnels $\mathbb{Q}$.

II. On considère le polynôme

$$P(X) = X^4 + X^3 - X^2 - X + 1 \in \mathbb{Q}[X].$$

1) a) Soit $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ un corps à 2 éléments et dans un clôture algébrique de $\mathbb{F}_2$, soit a tel que $a^2 + a + 1 = 0$. Montrer que $\mathbb{F}_2(a)$ est une extension de degré 2 de $\mathbb{F}_2$.

b) Soit $\overline{P}(X) \in \mathbb{F}_2[X]$ le polynôme $P(X)$ dont on a réduit les coefficients modulo 2. Montrer que $\overline{P}(X)$ n'a pas de racine dans $\mathbb{F}_2$ et $\mathbb{F}_2(a)$.

c) Montrer que $\overline{P}(X)$ est irréductible dans $\mathbb{F}_2[X]$.

d) En déduire que $P(X)$ est irréductible dans $\mathbb{Q}[X]$.

2) Soit L un corps de décomposition de $P(X)$ sur $\mathbb{Q}$ et soit $\theta \in L$ une racine de $P(X)$.

a) Montrer que $i\sqrt{3}$ est dans $\mathbb{Q}(\theta)$ (on pourra remarquer que dans $\mathbb{C}[X]$, $P(X) = (X^2 + ((1 + i\sqrt{3})/2)X\ - 1)(X^2 + ((1 - i\sqrt{3})/2)X\ - 1))$.

b) Montrer que $L/\mathbb{Q}$ est une extension de degré 8.

III. Soient p un nombre premier, avec $p \neq 2$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ un corps à p éléments, $K = \mathbb{F}_p(T)$ un corps de fractions rationnelles à une indéterminée et à coefficients dans $\mathbb{F}_p$. Soit

$$P(X) = X^{p^2} + (T - 1)X^p + T \in K[X].$$

Soit L un corps de décomposition de $P(X)$ sur K et soit θ une racine de $P(X)$ dans L.

1) Montrer que $P(X)$ est un élément irréductible de $K[X]$ (on pourra regarder ce polynôme dans $\mathbb{F}_p[T, X] = (\mathbb{F}_p[X])[T]$).

2) a) Ecrire le polynôme minimal de θ^p sur K, polynôme que l'on désignera par $Q(X)$.

b) Quel est le degré de séparabilité de $K(\theta)$ sur K ?

c) Décrire la sous-extension séparable maximale de $K(\theta)/K$.

3) Soit un élément z d'une clôture algébrique de L tel que

$$z^{p(p-1)} = 1 - T.$$

a) Montrer que les racines de $P(X)$ sont de la forme

$$\theta + \lambda z \quad \text{où} \quad \lambda \in \mathbb{F}_p.$$

b) En déduire que $z \in L$, que $L = K(\theta, z)$.

c) Décrire le groupe de Galois de L sur K ; on notera G ce groupe.

4) a) Montrer que $K(z^{p-1})/K$ est une extension purement inséparable de degré p.

b) Montrer que

$$\theta^p - z^{p-1}\theta \notin K(z^{p-1}).$$

(on pourra écrire $\theta^p - z^{p-1}\theta = \sum_{0 \le i \le p-1} u_i z^{(p-1)i}$, avec u_i dans K, élever à la puissance p, prendre les dérivées successives et ainsi obtenir que $u_i = 0$ pour $i > 1 \ldots$).

c) En déduire que $K(z^{p-1}, \theta^p - z^{p-1}\theta)$ est une extension purement inséparable de K de degré p^2.

d) En déduire que

$$L^G = K(z^{p-1}, \theta^p - z^{p-1}\theta),$$

où L^G est le sous-corps de L formé par ses éléments invariants sous l'action de $G = \mathrm{Gal}(L/K)$.

Examen partiel du 22 novembre 2000

I. Soient, dans $\mathbb{C}$, $\alpha = \sqrt{2}$ une racine de $X^2 - 2$ et $\beta = \sqrt[3]{3}$ la racine réelle de $X^3 - 3$.

1) a) Montrer que $\beta \notin \mathbb{Q}(\alpha)$, en déduire que $X^3 - 3$ est irréductible sur $\mathbb{Q}(\alpha)$.

b) Montrer que le corps $K = \mathbb{Q}(\alpha, \beta)$ est une extension de degré 6 de $\mathbb{Q}$.

2) Soit $H = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

a) Soit $\sigma \in H$, expliquer pourquoi σ est complètement déterminé par le couple $(\sigma(\alpha), \sigma(\beta)$. Donner la liste de toutes les valeurs possibles de ce couple.

3) Montrer que $K = \mathbb{Q}(\alpha + \beta)$ (on pourra compter les images distinctes de $\alpha + \beta$ par les éléments de H).

4) a) Montrer que le corps $L = \mathbb{Q}(\beta, j)$, où $j \neq 1$ est une racine cubique de l'unité dans $\mathbb{C}$, est un corps de décomposition de $X^3 - 3$ sur $\mathbb{Q}$.

b) Soit $F = K(j) = \mathbb{Q}(\alpha, \beta, j)$. Montrer que F est une extension normale de $\mathbb{Q}$, de degré 12.

5) a) Soit $\sigma \in H$ (cf question 2)) . Expliquer pourquoi il existe deux prolongements de σ (que l'on notera τ_1 et τ_2) en des automorphismes de F.

b) Montrer que $F = \mathbb{Q}(\alpha + \beta + j)$ (on pourra utiliser la question 3)).

II. Soit $K = \mathbb{F}_p(T)$ un corps des fractions rationnelles à une indéterminée et à coefficients dans $\mathbb{F}_p = \mathbb{Z}/pZ$ (où p est un nombre premier). Soit

$$P(X) = X^{p^2} - X^p - T \ \in \ K[X].$$

1) a) Montrer que $P(X)$ est irréductible sur K (on pourra considérer $P(X)$ comme un élément de $\mathbb{F}_p[X][T]$).

b) Soit θ une racine de $P(X)$, dans une clôture algébrique fixée $K^{\text{alg.}}$ de K. Montrer que les racines de $P(X)$ sont les $\theta + \lambda$, où λ décrit $\mathbb{F}_p$.

c) Soit $L = K(\theta)$, montrer que L est une extension normale de K.

2) Soit $G = \text{Gal}(L/K)$ et soit L^G l'ensemble des éléments de L invariants sous l'action de G.

a) Montrer que L^G est une extension de degré p de K.

b) Soit $\alpha \in K^{\text{alg.}}$ tel que $\alpha^p = T$. Montrer que $L^G = K(\alpha)$.

c) Quel est le degré de séparabilité de L sur K ?

3) Soit L_s le sous corps de L formé par ses éléments séparables sur K. Montrer que $L_s = K(\theta^p)$.

Examen du 30 janvier 2001

I. Soit

$$P(X) = X^4 + aX^2 + bX + c,$$

où a, b et c sont des éléments de $\mathbb{Q}$. On suppose que $P(X)$ est un élément irréductible de $\mathbb{Q}[X]$ et qu'il possède exactement deux racines réelles, notées α et α', on suppose de plus que

$$\alpha + \alpha' \neq 0.$$

Soient β et β' les deux autres racines de $P(X)$, dans $\mathbb{C}$. Soit L le sous-corps de $\mathbb{C}$ qui est un corps de décomposition de $P(X)$ sur $\mathbb{Q}$. On pose $G = \text{Gal}(L/\mathbb{Q})$.

1) Montrer que $[L : \mathbb{Q}(\alpha, \alpha')] = 2$, que $[\mathbb{Q}(\alpha, \alpha') : \mathbb{Q}(\alpha)]$ est égal à 1 ou 3. En déduire que $[L : \mathbb{Q}]$ est égal à 8 ou à 24, que $[L : \mathbb{Q}] = 8$ si et seulement si $\mathbb{Q}(\alpha, \alpha') = \mathbb{Q}(\alpha)$.

2) Soit $\varphi : G \to S_4$ l'application qui à tout élément σ de G associe la permutation obtenue par restriction de σ à $\{\alpha, \alpha', \beta, \beta'\}$.

a) Soit $G_1 = \text{Gal}(L/\mathbb{Q}(\alpha + \alpha'))$. Montrer que

$$\varphi(G_1) \subset \{\text{id}, (\alpha, \alpha'), (\beta, \beta'), (\alpha, \alpha')(\beta, \beta')\}$$

((α, α') désigne la transposition qui échange α et α', etc.).

b) Le temps de cette question on pose $t = \alpha + \alpha'$. En examinant les coefficients de $P(X)$ montrer que

$(\alpha\alpha') + (\beta\beta') - t^2 = a$,

$(-(\alpha\alpha') + (\beta\beta'))t = -b$,

$(\alpha\alpha')(\beta\beta') = c$.

En déduire que

$$t^6 + 2at^4 + (a^2 - 4c)t^2 - b^2 = 0.$$

c) Montrer que $[\mathbb{Q}(\alpha + \alpha') : \mathbb{Q}]$ est égal à 2, 4 ou 6.

3) Dans cette question on considère le polynôme

$$P(X) = X^4 + X^2 + X - 2,$$

c'est à dire que l'on pose $a = 1$, $b = 1$ et $c = -2$. On admet que $P(X)$ a deux racines réelles exactement, dont la somme est non nulle (ce n'est pas difficile à montrer).

a) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$ (on pourra examiner $P(X)$ modulo 3).

b) Montrer que L est une extension galoisienne de $\mathbb{Q}$ de degré 24 (soit $Q(X) = X^6 + 2X^4 + 9X^2 - 1$, cf question 2-b), on pourra examiner ce polynôme modulo 2).

c) Montrer que $\mathbb{Q}(\beta - \beta')$ est une extension de $\mathbb{Q}$, de degré 12 (on pourra examiner l'extension $L/\mathbb{Q}(\beta - \beta')$).

II. Soient p un nombre premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $K = \mathbb{F}_p(T)$ un corps de fractions rationnelles. On note K^{alg} une clôture algébrique de K. Soit

$$P(X) = X^{p^3} - (T^{p-1} - 1)X^{p^2} + T + 1 \in K[X] \ .$$

On désigne par α une racine de $P(X)$ dans K^{alg}.

1) a) Montrer que $P(X)$ est irréductible dans $K[X]$.

b) Montrer qu'il existe un polynôme $Q(X)$ de $K[X]$, irréductible, tel que $P(X) = Q(X^{p^2})$.

c) Montrer qu'il existe un corps intermédiaire M, $K \subset M \subset K(\alpha)$, tel que l'extension M/K soit séparable et que l'extension $K(\alpha)/M$ soit purement inséparable. Donner les degrés de ces deux extensions. Décrire M.

2) a) Soient β et γ, deux éléments de K^{alg} tels que

$$\beta^{p^2} = T^{p-1} - 1 \ \text{ et } \ \gamma^{p-1} = \beta \ .$$

Montrer que les racines de $P(X)$ sont les $\alpha + \lambda\gamma$, où λ décrit $\mathbb{F}_p$.

b) Montrer que

$$\mathrm{irr}(\beta, K; X) = \mathrm{irr}(\beta, M; X) = X^{p^2} - (T^{p-1} - 1).$$

c) Soit $d = [K(\alpha, \beta)/K(\alpha)]$, montrer que d est un diviseur de p^2.

d) Montrer que l'extension $K(\gamma^{p^2})/K$ est galoisienne, de groupe de Galois isomorphe à $\mathbb{F}_p^*$.

e) En déduire que l'extension $K(\alpha,\gamma)/K(\alpha,\beta)$ est aussi galoisienne de groupe de Galois isomorphe à $\mathbb{F}_p^*$ (on pourra utiliser que, suivant la question précédente, $p-1$ divise $[K(\alpha,\gamma):K]$).

3) a) Montrer que $K(\alpha,\gamma)$ est un corps de décomposition de $P(X)$ sur K, que $[K(\alpha,\gamma):K]_s = p(p-1)$.

b) Soit

$$G = \mathrm{Gal}(K(\alpha,\gamma)/K),$$

établir la formule

$$K(\alpha,\gamma)^G = K(\alpha^p - \beta\alpha, \beta).$$

4) a) Montrer que l'extension $K(\alpha^{p^2},\gamma^{p^2})/K$ est galoisienne, de degré $p(p-1)$.

b) Soit $G_1 = \mathrm{Gal}(K(\alpha^{p^2},\gamma^{p^2})/K)$ et soit $\sigma \in G_1$. Montrer qu'il existe $\lambda \in \mathbb{F}_p$ et $\mu \in \mathbb{F}_p^*$ tels que

$$\sigma(\alpha^{p^2}) = \alpha^{p^2} + \lambda\gamma^{p^2} \quad , \quad \sigma(\gamma^{p^2}) = \mu\gamma^{p^2}.$$

c) Soit H le sous-groupe de $\mathrm{GL}_2(\mathbb{F}_p)$ ainsi défini :

$$H = \{\begin{pmatrix} \mu & \lambda \\ 0 & 1 \end{pmatrix} \ / \ \lambda \in \mathbb{F}_p \ , \ \mu \in \mathbb{F}_p^*\}.$$

Montrer que G_1 et H sont isomorphes.

d) Montrer que le groupe G est isomorphe à H.

e) Calculer le degré de $K(\alpha,\beta)$ sur $K(\alpha^p - \beta\alpha, \beta)$. Cette extension est-elle galoisienne ?

Examen du 10 septembre 2001

I. On désigne par $\mathbb{F}$ le corps $\mathbb{Z}/13\mathbb{Z}$ et soit $P(X) = X^2 - 2 \in \mathbb{F}[X]$.

1) Montrer que $P(X)$ est irréductible dans $\mathbb{F}[X]$.

2) Dans une clôture algébrique de $\mathbb{F}$ soit θ une racine de $P(X)$ et soit $K = \mathbb{F}(\theta)$. Montrer que tout polynôme $Q(X)$ de $\mathbb{F}[X]$, de *degré 2*, a une racine dans K.

II. Soit $P(X) = X^4 + 9X^2 + 1 \in \mathbb{Q}[X]$. On pourra remarquer que $P(X) = (X^2 - i\sqrt{7}X + 1)(X^2 + i\sqrt{7}X + 1)$ dans $\mathbb{C}[X]$.

1) a) Montrer que $P(X)$ est irréductible sur $\mathbb{Q}$.

b) Montrer que le corps de décomposition de $P(X)$ dans $\mathbb{C}$ est $K = \mathbb{Q}(i\sqrt{7} \ , \ i\sqrt{11})$.

2) Soit G le groupe de Galois de K sur $\mathbb{Q}$.

a) Montrer que G est d'ordre 4.

b) Montrer que G possède deux éléments, notés σ et τ, tels que

$$\sigma(i\sqrt{7}) = -i\sqrt{7},\ \ \sigma(i\sqrt{11}) = i\sqrt{11},$$

$$\tau(i\sqrt{7}) = i\sqrt{7},\ \ \tau(i\sqrt{11}) = -i\sqrt{11}.$$

3) Soit $\alpha = i\sqrt{7} + i\sqrt{11}$, montrer que $K = \mathbb{Q}(\alpha)$.

III. Soient p un nombre premier différent de 2 et $K = \mathbb{F}_p(T)$ un corps des fractions rationnelles à une indéterminée et à coefficients dans $\mathbb{F}_p = \mathbb{Z}/pZ$. Soit

$$P(X) = X^{p^3} - (T^{p^2} + 2)X^{p^2} + T + 2 \in K[X].$$

1) a) Montrer que $P(X)$ est irréductible sur K.

b) Soit θ une racine de $P(X)$, dans une clôture algébrique fixée $K^{\text{alg.}}$ de K. Soit $L = K(\theta)$ et soit L_s le plus grand sous-corps de L qui soit une extension séparable de K. Montrer $L_s = K(\theta^{p^2})$.

2) On se place dans $K^{\text{alg.}}$.

a) Montrer que les racines de $P(X)$ sont les $\theta + u$, où u décrit l'ensemble des racines du polynôme $X^p - (T+2)X$.

b) Soit u_0 une racine non nulle de $X^p - (T+2)X$, montrer que l'ensemble des racines de ce polynôme est $\{\lambda u_0 \ / \ \lambda \in \mathbb{F}_p\}$.

c) Montrer que l'extension $K(u_0)/K$ est cyclique de degré $p-1$.

d) En déduire que l'extension $L(u_0)/L$ est cyclique de degré $p-1$.

3) a) On pose $F = L(u_0) = K(\theta, u_0)$. Montrer que F est un corps de décomposition de $P(X)$ sur K.

b) Soit G le groupe de Galois de F sur K. Soit λ un générateur de $\mathbb{F}_p^*$. Montrer que G est engendré par deux éléments σ et τ dont les définitions sont

$$\sigma(\theta) = \theta\ ,\ \sigma(u_0) = \lambda u_0,$$

$$\tau(\theta) = \theta + u_0\ ,\ \tau(u_0) = u_0.$$

4) Soit F^G le corps des invariants de F par G. Montrer que l'extension F^G/K est de degré p^2, que $F^G = K(\theta^p - (T+2)\theta)$.

Examen partiel, octobre 2001.

I. Soit $P(X) = X^3 - 5 \in \mathbb{Q}[X]$.

1) Montrer $\mathbb{Q}(\sqrt[3]{5})$ est une extension de degré 3 de $\mathbb{Q}$.

2) Soit $j \in \mathbb{C}$ une racine cubique de l'unité, $j \neq 1$. Montrer que $\mathbb{Q}(\sqrt[3]{5}, j)$ est une extension de degré 6 de $\mathbb{Q}$.

3) On pose

$$H_1 = \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{5}), \mathbb{C}) \quad \text{et} \quad H_2 = \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{5}, j), \mathbb{C}).$$

a) Montrer que H_1 possède trois éléments, notés s_1, s_2 et s_3, ainsi caractérisés :

$$s_1(\sqrt[3]{5}) = \sqrt[3]{5}\ ,\ s_2(\sqrt[3]{5}) = j\sqrt[3]{5}\ ,\ s_3(\sqrt[3]{5}) = j^2\sqrt[3]{5}.$$

b) Montrer que H_2 possède 6 éléments, notés $\tau_{i,k}$, $i = 1, 2, 3$ et $k = 1, 2$, complètement déterminés par les formules

$$\tau_{i,k} \mid \mathbb{Q}(\sqrt[3]{5}) = s_i \quad \text{et} \quad \tau_{i,k}(j) = j^k.$$

c) Expliquez pourquoi les éléments de H_2 sont des $\mathbb{Q}$-automorphismes de $\mathbb{Q}(\sqrt[3]{5}, j)$.

3) Soit $\theta = \sqrt[3]{5} + j$, en examinant les images de θ par les éléments de H_2, montrer que $\mathrm{irr}(\theta, \mathbb{Q}; X)$ est de degré au moins 6. En déduire que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[3]{5}, j)$.

II. Soient p un nombre premier et $K = \mathbb{F}_p(T)$ un corps des fractions rationnelles à une indéterminée et à coefficients dans $\mathbb{F}_p = \mathbb{Z}/pZ$. Soit $P(X) = X^p - T \in K[X]$. Soit θ une racine de $P(X)$, dans une clôture algébrique fixée K^{alg} de K.

1) a) Montrer que $P(X)$ est irréductible sur K.

b) Quelles sont les racines de $P(X)$ dans K ?

c) Décrire les prolongements à $K(\theta)$ du morphisme inclusion $K \subset K^{\mathrm{alg}}$.

2) Soit l un nombre premier, $l \neq p$ et soit $Q(X) = X^l - \theta \in K(\theta)[X]$.

a) Montrer que $Q(X)$ est irréductible sur $K(\theta)$.

b) Soit ζ une racine de $Q(X)$ dans K^{alg}. Montrer que $K(\theta, \zeta)$ est une extension normale de K.

c) Combien l'inclusion $K \subset K^{\mathrm{alg}}$ admet-elle de prolongement à $K(\theta, \zeta)$?

Examen partiel du 12 novembre 2001

Pour alléger l'écriture, on pose $\alpha = \sqrt[4]{3}$ et $\beta = \sqrt[3]{2}$.

1. Montrer que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est de degré 4.

2. Montrer que $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ est de degré 12.

3. Soit $L = \mathbb{Q}(\alpha, \beta, i)$, où i est un élément de $\mathbb{C}$ tel que $i^2 = -1$. Montrer que L est une extension normale de $\mathbb{Q}$, de degré 24.

4. Soient $E = \mathbb{Q}(\beta, j)$, où $j \in \mathbb{C}$ est une racine cubique non triviale de l'unité. Montrer que $E/\mathbb{Q}$ est une extension normale.

5. Soient $H = \mathrm{Gal}(E/\mathbb{Q})$, a et b les éléments de H ainsi définis :

$$a(\beta) = j\beta\ \ ,\ \ a(j) = j \quad \text{et} \quad b(\beta) = \beta\ \ ,\ \ b(j) = j^2\ .$$

Expliquer pourquoi a et b existent. Montrer qu'il existe un isomorphisme φ de H avec le groupe S_3 des permutations d'un ensemble à 3 éléments, tel que $\varphi(a) = (1,2,3)$ et $\varphi(b) = (1,2)$.

6. Montrer que L est une extension de E, normale et de degré 4. Soit $N = \mathrm{Gal}(L/E)$, donner la structure de N (montrer que c'est un groupe abélien possédant trois éléments d'ordre 2...).

7. Soient $G = \mathrm{Gal}(L/\mathbb{Q})$ et

$$r : \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C}) \longrightarrow \mathrm{Hom}_{\mathbb{Q}}(E, \mathbb{C})$$

la restriction à E des $\mathbb{Q}$-homomorphismes de L dans $\mathbb{C}$. Expliquer pourquoi r induit un homomorphisme de groupes $R : G \to H$. Expliquer aussi pourquoi R est surjectif.

8. Montrer qu'il existe σ et τ appartenant à G tels que (cf. question 4))

$$R(\sigma) = a \ \ , \ \ \sigma(\alpha) = \alpha \quad \text{et} \quad R(\tau) = b \ \ , \ \ \tau(\alpha) = \alpha \ .$$

Montrer que

$$G = \{\sigma^n \tau^m \mu \ / \ n = 0,1,2 \ \ m = 0,1 \ \ \mu \in N\}.$$

Examen du 18/01/02.

I. Soient a et b deux entiers et

$$P(X) = X^4 + aX + b \in \mathbb{Z}[X].$$

On suppose que a et b vérifient

$$a \equiv b \equiv 1 \ \mathrm{mod.}2 \ \ , \ \ a \equiv b \equiv 1 \ \mathrm{mod.}3.$$

Soient L le corps de décomposition sur $\mathbb{Q}$ de $P(X)$ contenu dans $\mathbb{C}$ et A la fermeture intégrale de $\mathbb{Z}$ dans L. Si p est un nombre premier, on désigne par $\mathfrak{P}_p$ un idéal premier de A au dessus de l'idéal $p\mathbb{Z}$ de $\mathbb{Z}$.

On pose $G = \mathrm{Gal}(L/\mathbb{Q})$. Soit

$$\mathcal{Z} = \{\alpha_i \ / \ i = 1,2,3,4\} \subset L$$

l'ensemble des racines de $P(X)$ dans L. On sait que les éléments de G induisent des permutations de $\mathcal{Z}$, ce qui autorise à utiliser le vocabulaire de ces dernières : on dit de certains éléments de G que ce sont des cycles, des transpositions etc. quand ils le sont sur $\mathcal{Z}$.

1) Montrer que $P(X)$ est irréductible sur $\mathbb{Q}$ et que G possède un cycle d'ordre 4, que l'on notera σ (on pourra regarder $P(X)$ modulo 2).

2) Soit $\mathfrak{P}_3$ un idéal premier de A au dessue de $3\mathbb{Z}$. Décrire le groupe de décomposition de $\mathfrak{P}_3$, noté $G_{\mathfrak{P}_3}$, en déduire que G possède un cycle d'ordre 3, que l'on notera τ.

3) Montrer que G est isomorphe au groupe des permutations S_4 (on pourra d'abord montrer que G contient tous les cycles d'ordre 3).

4) a) Soit

$$d = \prod_{i \neq j} (\alpha_i - \alpha_j)$$

$(i, j \in \{1, 2, 3, 4\})$. Montrer que d est un élément de $\mathbb{Z}$.

b) Trouver δ dans L tel que $\delta^2 = d$ et montrer que $\delta \notin \mathbb{Q}$.

c) Soit $H = \mathrm{Gal}(L/\mathbb{Q}(\delta))$, montrer que H est isomorphe au groupe alterné A_4.

5) Soit $K = L^{G_{\mathfrak{P}_3}}$, le corps des invariants sous l'action de $G_{\mathfrak{P}_3}$ (cf. question 2). Montrer qu'il existe une racine α de $P(X)$ (dans L) telle que $K = \mathbb{Q}(\alpha, \delta)$.

II. Soient $p > 2$ un nombre premier et $K = \mathbb{F}_{p^2}(T)$ un corps des fractions rationnelles à une indéterminée et à coefficients dans le corps $\mathbb{F}_{p^2}$ (corps à p^2 éléments). Soit

$$P(X) = X^{p^3} - T^2 X^p + T \ \in \ K[X].$$

Soit θ une racine de $P(X)$, dans une clôture algébrique fixée K^{alg} de K. Soient α et β deux éléments de K^{alg} tels que

$$\alpha^p = T^2 \quad \text{et} \quad \beta^{p^2-1} = \alpha.$$

1) a) Montrer que $P(X)$ est irréductible sur K.

b) Montrer que l'ensemble des racines de $P(X)$ dans K^{alg} est

$$\{\theta + \lambda\beta \ / \ \lambda \in \mathbb{F}_{p^2}\}.$$

c) Décrire les prolongements à $K(\theta)$ du morphisme inclusion $K \subset K^{\mathrm{alg}}$.

d) Quel le degré d'inséparabilité de $K(\theta)$ sur K ? Décrire la sous-extension séparable maximale de $K(\theta)/K$.

2) a) Montrer qu'il existe $\gamma \in K(\alpha)$ tel que $\gamma^2 = \alpha$ (on pourra utiliser le fait que l'extension $K(\alpha, \gamma)/K$ est purement inséparable).

b) En déduire que α appartient à $K(\theta)$ (on pourra calculer $(\theta^{p^2} - \alpha\theta)^p$).

c) Montrer que $K(\theta) = K(\theta^p, \alpha)$.

3) a) Montrer que

$$\mathrm{irr}(\beta, K; X) = X^{p(p^2-1)/2} - T.$$

b) En déduire que l'extension $K(\beta)/K(\alpha)$ est de degré $(p^2 - 1)/2$.

c) Soit $L = K(\theta, \beta)$, montrer que c'est un corps de décomposition de $P(X)$ sur K et que $[L : K] = p^3(p^2 - 1)/2$.

4) Soit $G = \mathrm{Gal}(L/K)$.

a) Montrer que $\circ(G) = p^2(p^2 - 1)/2$.

b) Prouver que $L^G = K(\alpha)$.

5) Soit M l'ensemble des carrés non nuls de $\mathbb{F}_{p^2}$:

$$M = \{\lambda^2 \ / \ \lambda \in \mathbb{F}_{p^2}^*\}.$$

a) Soit $(\mu, \lambda) \in M \times \mathbb{F}_{p^2}$, montrer qu'il existe $\sigma_{(\mu,\lambda)} \in G$ tel que

$$\sigma_{(\mu,\lambda)}(\beta) = \mu\beta \quad \text{et} \quad \sigma_{(\mu,\lambda)}(\theta) = \theta + \lambda\beta \ .$$

b) En déduire que G est isomorphe au produit semi-direct du groupe multiplicatif M et du groupe additif $\mathbb{F}_{p^2}$, le premier opérant sur $\mathbb{F}_{p^2}$ par translations, c'est à dire

$$G \simeq M \ltimes \mathbb{F}_{p^2} \ ,$$

l'opération dans le membre de droite étant définie par

$$(\mu, \lambda)(\mu', \lambda') = (\mu\mu', \lambda + \mu\lambda').$$

Index

élément
    algébrique, 5, 6
    entier, 92, 93
    primitif, 37, 39
    purement inséparable, 34
    séparable, 30
    transcendant, 5
équation résoluble par radicaux, 81

anneau
    de fractions, 97, 98
    factoriel, 94
    noethérien, 94
    principal, 95, 96
Artin, Emile, 10, 66
Artin-Schreier, 67, 81, 82

caractéristique, 4, 5, 15
caractère, 42
Cardan, 74
clôture algébrique, 10, 13
    de $\mathbb{R}$, 68
    existence et unicité, 10
Cohen-Seidenberg, 99
compositum, 4, 21, 51, 52
corps, 1
    algébriquement clos, 10, 59
    de rupture, 9
    fini, 37, 62, 63
    groupe multiplicatif, 59
    parfait, 36, 37
corps de décomposition, 19, 20
    existence, 19
    unicité, 20
correspondance de Galois, 49

discriminant, 69, 74

extension abélienne, 66
extension cyclique, 66, 67
extension cyclotomique, 59, 61
    de $\mathbb{Q}$, 61
    degré, 61
extension de corps, 1
    algébrique, 5, 7, 9
    base, 2, 6
    de type fini, 4
    degré, 2, 6, 52
    engendrée, 3, 7
    finie, 2, 6, 7
    monogène, 28, 33, 37, 39
extension galoisienne, 49, 61, 103
extension inséparable, 30
extension normale, 21, 35
extension purement inséparable, 32, 34
extension quasi-galoisienne, voir extension normale
extension résoluble, 78, 81, 82
extension résoluble par radicaux, 81, 82
extension séparable, 30, 94, 96
    sous-extension séparable maximale, 32

fermeture intégrale, 93, 94, 96, 103
fermeture normale, 22, 23, 78
Ferrari, 75
forme bilinéaire, 41
Frobenius, 15, 36, 37, 64

groupe
    alterné, 77
    cyclique, 59

de décomposition, 101, 103
de permutations, 76
résoluble, 77, 79, 80
résolution, 79
groupe de Galois, 22, 35, 49, 51, 61, 78, 89, 103

homomorphisme de corps, voir morphisme de corps

indicateur d'Euler, 60, 61
inséparabilité, 27
degré, 28, 31
intégralement clos, 93, 94

Kummer, 67, 82

lemme d'Artin, 42, 66
lemme de Nakayama, 98
Liouville, 17

module, 55, 89
de torsion, 55, 90
de type fini, 90
morphisme, 90
factorisation, 90
noethérien, 91
quotient, 90
morphisme de corps, 1
automorphisme, 13
endomorphisme, 13
K-morphisme, 2

norme, 39, 40, 66

p-groupe, 69
centre, 69
polynôme
cyclotomique, 60, 61
irréductible, 5, 6, 40, 67
minimal, voir polynôme irréductible
séparable, 30, 103
prolongement
de morphisme, 10, 12, 27, 33, 41
des ideaux premiers, 99, 102

racine, 8, 9, 23, 69, 81
de l'unité, 59
primitive de l'unité, 60
radical de Jacobson, 98

séparabilité, 27
degré, 27, 31, 34, 35
monogène, 28
sous-corps premier, 5

théorème 90 de Hilbert, 66
théorème de Kronecker et Weber, 66
théorème de l'élément primitif, 37, 38
théorème de la base normale, 53
théorème de Wedderburn, 64
théorie de Galois, voir correspondance de Galois
trace, 39, 40, 44, 66