VII. EXTENSIONS DE CORPS : CARACTÉRISTIQUE, CORPS DE RUPTURE, CORPS DE DÉCOMPOSITION, CLÔTURES ALGÉBRIQUES

SÉANCES DU 23, 29 ET 30 OCTOBRE

15. Construction d'extensions de corps

15.1. Généralités sur les extensions de corps. — [(7)] Pour la commodité du lecteur, nous répétons dans ce paragraphe des définitions et résultats déjà énoncés dans le chapitre V.

Remarque 15.1. — Soient K et K′ deux corps et soit $\phi : \mathrm{K} \to \mathrm{K}'$ un morphisme d'anneaux. Alors :

a) ϕ est **injectif** car $\operatorname{Ker}\phi$, étant un idéal propre de K (car $\phi(1) = 1$), est nécessairement nul.

b) ϕ est un **morphisme de corps**, car l'égalité

$$1 = \phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$$

entraîne que $\phi(x^{-1}) = \phi(x)^{-1}$ pour tout $x \in \mathrm{K} \setminus \{0\}$.

Définition 15.2. — 1) On dit que K est une **extension** de k si l'on s'est donné un morphisme (nécessairement injectif) $k \to \mathrm{K}$. On utilise la notation « K/k » pour signifier que K est une extension de k (il est sous-entendu que k et K sont des corps). Parfois, on dira aussi que K est un **surcorps** de k.

2) Si K/k est une extension, une **extension intermédiaire** L est un corps L tel que $k \subseteq \mathrm{L} \subseteq \mathrm{K}$. Dans ce cas, on dit aussi que L/k est une **sous-extension** de K/k.

Lemme 15.3. — *Soit* K *un corps. Si* $(\mathrm{K}_i)_{i\in\mathrm{I}}$ *est une famille de sous-corps de* K*, alors l'intersection des* K_i *est un sous-corps de* K.

Démonstration. — Facile, et laissée au lecteur. □

[(7)] version du 4/11/07

***Définition 15.4* (Sous-corps engendré).** — 1) Soient K un corps et S une partie de K. L'ensemble des sous-corps de K contenant S est non-vide (car il contient K) et donc l'intersection de tous ces sous-corps est un sous-corps de K. C'est le plus petit sous-corps contenant S ; on l'appelle le sous-corps **engendré par** S.

2) On appelle **sous-corps premier** de K le sous-corps de K engendré par l'élément 1_{K}. Il est contenu dans tout sous-corps de K.

3) Soit K/k une extension de corps et soit S une partie de K. L'ensemble des sous-corps de K contenant k et S est non-vide (car il contient K) et donc l'intersection de tous ces sous-corps est un sous-corps de K, qui est le plus petit sous-corps contenant k et S. On l'appelle le sous-corps **engendré par** S **sur** k et on le note $k(\mathrm{S})$, ou $k(x_1, \ldots, x_n)$ si $\mathrm{S} = \{x_1, \ldots, x_n\}$.

***Définition 15.5* (Extensions de type fini).** — 1) On dit que K/k est une **extension de type fini** si K est engendré comme surcorps de k par un nombre fini d'éléments, c.-à-d., s'il existe $x_1, \ldots, x_n \in \mathrm{K}$ tels que $\mathrm{K} = k(x_1, \ldots, x_n)$.

2) On dit que K/k est une **extension monogène** si K est engendré sur k par un élément x, c.-à-d., s'il existe $x \in \mathrm{K}$ tel que $\mathrm{K} = k(x)$.

Lemme 15.6. — *Soit* K *un surcorps de* k *et soient* I, J *deux parties de* K. *Alors*

$$k(\mathrm{I} \cup \mathrm{J}) = k(\mathrm{I})(\mathrm{J}).$$

Par conséquent, toute extension de type fini $k \subset k(x_1, \ldots, x_n)$ *est obtenue comme composée d'extensions monogènes :*

$$k(x_1, \ldots, x_n) = k(x_1)(x_2, \ldots, x_n) = k(x_1)(x_2) \cdots (x_n).$$

Démonstration. — $k(\mathrm{I})(\mathrm{J})$ contient $\mathrm{I} \cup \mathrm{J}$ et donc $k(\mathrm{I} \cup \mathrm{J})$. Réciproquement, $k(\mathrm{I} \cup \mathrm{J})$ contient $k(\mathrm{I})$ et J, donc $k(\mathrm{I})(\mathrm{J})$. Ceci prouve le lemme. □

Remarque 15.7. — Dans ce cours, on ne considèrera que des extensions de type fini. Mais les extensions de type infini existent dans la nature. Par exemple, l'extension $\mathbb{Q} \subseteq \mathbb{R}$ n'est pas de type fini, car on peut montrer que $\mathbb{R}$ est de degré de transcendance (voir le paragraphe 15.9 plus bas) infini sur $\mathbb{Q}$.

Définition 15.8. — Soient K et K′ deux extensions de k. On dit que K et K′ sont k**-isomorphes** s'il existe un isomorphisme $\phi : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$ (de corps ou d'anneaux ; on a vu que c'était la même chose) tel que $\phi(\lambda) = \lambda$ pour tout $\lambda \in k$. Ceci équivaut à dire que ϕ est un isomorphisme de k-algèbres.

Plus généralement, si, plutôt qu'une inclusion de k dans K et K′, on s'est donné des morphismes de corps

$$\tau : k \hookrightarrow \mathrm{K} \qquad \text{et} \qquad \tau' : k \hookrightarrow \mathrm{K}',$$

alors un k**-morphisme** de K vers K′ est un morphisme $\phi : \mathrm{K} \to \mathrm{K}'$ tel que $\phi \circ \tau = \tau'$.

15.2. Sous-corps premier et caractéristique. — Il y a deux exemples fondamentaux de corps. D'une part, le corps des rationnels $\mathbb{Q}$, qui est le corps des fractions de $\mathbb{Z}$. D'autre part, les corps finis $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}_p$, où $p \in \mathbb{Z}$ est un nombre premier.

Définition 15.9. — Soit $p \geqslant 2$ un nombre premier. On note $\mathbb{F}_p$ l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$. C'est un corps car l'idéal $p\mathbb{Z}$ est maximal, puisque $\mathbb{Z}$ est principal et p irréductible.

De façon équivalente, mais plus concrète, le fait que $\mathbb{Z}/(p)$ soit un corps résulte du théorème de Bezout. En effet, soit $a \in \mathbb{Z}$ non divisible par p. Comme l'idéal engendré par a et p est $\mathbb{Z}$, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha a + \beta p = 1$. Alors, les classes de α et a modulo p sont inverses l'une de l'autre.

En pratique, on peut trouver explicitement les « coefficients de Bezout » α et β (et donc l'inverse α de a modulo p), par la méthode des divisions successives.

Exemples 15.10. — **1)** Prenons $p = 37$ et $a = 7$. Alors

$$\begin{cases} 37 = 5 \times 7 + 2 \\ 3 \times 2 + 1 = 7, \end{cases} \quad \text{d'où} \quad \begin{cases} 3 \cdot 37 = 15 \times 7 + 3 \times 2 \\ 3 \times 2 + 1 = 7, \end{cases}$$

et $16 \cdot 7 - 3 \cdot 37 = 1$. Donc l'inverse de 7 mod. 37 est 16.

2) Prenons $p = 167$ et $a = 17$. Alors

$$\begin{cases} 167 = 9 \times 17 + 14 \\ 14 + 3 = 17 \\ 14 = 4 \times 3 + 2 \\ 1 + 2 = 3, \end{cases} \quad \text{d'où} \quad \begin{cases} 14 + 1 = 5 \times 3, \\ 6 \times 14 + 1 = 5 \times 17, \\ 6 \times 167 + 1 = (6 \cdot 9 + 5) \times 17. \end{cases}$$

Donc $1 = 59 \cdot 17 - 6 \cdot 167$ et 59 est l'inverse de 17 modulo 167.

Lemme 15.11. — *Soit* A *un anneau. Il existe un unique morphisme d'anneaux* $\phi : \mathbb{Z} \to \mathrm{A}$.

Démonstration. — Comme A est un groupe abélien, c'est un $\mathbb{Z}$-module, pour l'action définie, pour tout $n \geqslant 0$ et $x \in \mathrm{A}$, par $n \cdot x = x + \cdots + x$ (n fois), et $(-n) \cdot x = n \cdot (-x)$. De plus, le morphisme de $\mathbb{Z}$-modules $\phi : \mathbb{Z} \to \mathrm{A}$, $n \mapsto n \cdot 1$ est un morphisme d'anneaux, puisque la distributivité de la multiplication dans A entraîne :

$$(m \cdot 1)(n \cdot 1) = (1 + \cdots + 1)(1 + \cdots + 1) = (mn) \cdot 1.$$

Ceci prouve l'existence. Réciproquement, si $\psi : \mathbb{Z} \to \mathrm{A}$ est un morphisme d'anneaux, alors $\psi(1) = 1$ et $\psi(n) = n \cdot 1$ pour tout $n \in \mathbb{Z}$, donc $\psi = \phi$. □

Rappelons la définition suivante, déjà introduite en 15.4.

Définition 15.12. — On appelle **sous-corps premier** de K le sous-corps de K engendré par l'élément 1_{K}. Il est contenu dans tout sous-corps de K.

Théorème 15.13 **(Caractéristique et sous-corps premier)**
Soit K *un corps. Son sous-corps premier est isomorphe soit à* $\mathbb{Q}$*, soit à* $\mathbb{F}_p$*, pour un nombre premier* $p \geqslant 2$ *uniquement déterminé. On dit que la* **caractéristique** *de* K *est* 0 *dans le premier cas, et* p *dans le second cas.*

De façon plus précise, la caractéristique de K *est le générateur* $\geqslant 0$ *du noyau du morphisme* $\mathbb{Z} \to \mathrm{K}$, $n \mapsto n \cdot 1_{\mathrm{K}}$. *On la note* $\mathrm{car}(\mathrm{K})$.

Démonstration. — Soit ϕ l'unique morphisme d'anneaux $\mathbb{Z} \to \mathrm{K}$. Alors $\operatorname{Ker}\phi$ est un idéal premier de $\mathbb{Z}$, puisque $\mathbb{Z}/\operatorname{Ker}\phi$ est isomorphe à un sous-anneau de K, donc intègre. Par conséquent, de deux choses l'une.

1) Si $\operatorname{Ker}\phi = (0)$, on peut identifier $\mathbb{Z}$ à son image $\mathbb{Z}1_{\mathrm{K}}$. Comme tout élément de $\phi(\mathbb{Z} \setminus \{0\})$ est inversible dans K, alors ϕ se prolonge en un morphisme d'anneaux $\psi : \mathbb{Q} \to \mathrm{K}$, nécessairement injectif puisque $\mathbb{Q}$ est un corps. De plus, tout sous-corps de K contient 1_{K}, les éléments $n \cdot 1_{\mathrm{K}}$ et leurs inverses. Ceci montre que le sous-corps premier de K est $\psi(\mathbb{Q})$, isomorphe à $\mathbb{Q}$. Dans ce cas, on identifiera $\mathbb{Q}$ à son image dans K :

$$\mathbb{Q} = \{x \in \mathrm{K} \mid \exists\, n, m \in \mathbb{Z}, n \neq 0, \text{ tels que } nx = m1_{\mathrm{K}}\}.$$

2) Si $\operatorname{Ker}\phi \neq (0)$, alors $\operatorname{Ker}\phi = (p)$, où p est un nombre premier $\geqslant 2$ uniquement déterminé. Dans ce cas, ϕ induit un isomorphisme de $\mathbb{F}_p$ sur son image, qui est formée des éléments $n1_{\mathrm{K}}$ pour $0 \leqslant n < p$. Ceci montre que, dans ce cas, le sous-corps premier de K est formé des éléments $n1_{\mathrm{K}}$ pour $0 \leqslant n < p$; on l'identifiera à $\mathbb{F}_p$. Le théorème est démontré. □

Enfin, notons la proposition suivante, facile mais extrêmement importante.

Proposition 15.14. — *Soient* $k \subseteq \mathrm{K}$ *deux corps. Alors* k *et* K *ont la même caractéristique.*

Démonstration. — k et K ont même sous-corps premier. □

15.3. Endomorphismes de Frobenius. — Signalons, dans ce paragraphe, une propriété particulière des corps k de caractéristique $p > 0$; dans ce cas, on a :

$$(*) \qquad (a+b)^p = a^p + b^p, \qquad \forall\, a, b \in k.$$

Pour démontrer ceci, commençons par quelques rappels sur les coefficients binomiaux et la formule du binôme (dûe à Pascal).

Définition 15.15. — Soient i, n deux entiers tels que $0 \leqslant i \leqslant n$. On rappelle la définition du coefficient binomial :

$$\binom{n}{i} := \frac{n!}{i!(n-i)!}.$$

(On le note aussi C_n^i.) C'est le nombre de façons de choisir i éléments dans un ensemble à n éléments. Pour $i = 0$ ou n, ceci vaut 1.

On rappelle la formule de Pascal (pour $i \geqslant 1$) :

$$\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1},$$

qu'on obtient en remarquant que, quand on prend i éléments dans $\{1, \dots, n\}$, on peut ou bien prendre, ou ne pas prendre, n.

On rappelle aussi la formule du binôme, valable dans tout anneau commutatif.

Lemme 15.16 **(Formule du binôme)**. — *Soient* A *un anneau commutatif et* $a, b \in \mathrm{A}$. *Pour tout* $n \geqslant 1$, *on a :*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Démonstration. — Par récurrence sur n, en utilisant la formule de Pascal. □

Lemme 15.17. — *Soit* $p \in \mathbb{N}$ *un nombre premier. Alors* p *divise* $\binom{p}{i}$ *pour tout* $i = 1, \dots, p-1$.

Démonstration. — p divise $p! = i!(p-i)!\binom{p}{i}$ et est premier avec $i!(p-i)!$, donc divise $\binom{p}{i}$. □

Corollaire 15.18. — *Soient* k *un corps de caractéristique* $p > 0$ *et* A *une* k*-algèbre commutative. Alors,*

$$(a+b)^p = a^p + b^p, \qquad \forall\, a, b \in \mathrm{A}.$$

Démonstration. — Ceci résulte de la formule du binôme et du lemme précédent. □

En particulier, on obtient la proposition suivante.

Proposition 15.19 **(L'endomorphisme de Frobenius** Fr_p**)**. — *Soit* K *un corps de caractéristique* $p > 0$. *Alors l'application* $x \mapsto x^p$ *est un endomorphisme du corps* K, *noté* Fr_p. *De plus, si* K *est fini, alors* Fr_p *est un automorphisme de* K.

Démonstration. — Il est clair que $1^p = 1$ et $(ab)^p = a^p b^p$ pour tout $a, b \in \mathrm{K}$, et l'on vient de voir l'égalité $(a+b)^p = a^p + b^p$.

Donc, Fr_p est un morphisme de corps de K vers K, c.-à-d., un endomorphisme de corps de K. Il est bien sûr injectif, comme tout morphisme de corps. Par conséquent, si K est fini, Fr_p est bijectif donc un automorphisme de K. □

Corollaire 15.20 **(Les endomorphismes de Frobenius $\mathrm{Fr}_q = \mathrm{Fr}_{p^n}$)**

Soient K *un corps de caractéristique* $p > 0$ *et* $n \geqslant 1$. *L'application* $\mathrm{Fr}_p^n := \mathrm{Fr}_p \circ \cdots \circ \mathrm{Fr}_p$ (n *fois*), *qui à tout* x *associe* x^{p^n}, *est un endomorphisme du corps* K. *On le note aussi* Fr_{p^n} *ou* Fr_q *si* $q = p^n$. *Si* K *est fini, c'est un automorphisme de* K.

Démonstration. — Ceci résulte immédiatement de la proposition précédente. □

Corollaire 15.21. — *Soient* p *un nombre premier,* $n \geqslant 1$ *et* $q = p^n$. *Alors* p *divise* $\binom{q}{i}$ *pour tout* $i = 1, \ldots, q-1$.

Démonstration. — Plaçons-nous dans le corps $\mathrm{K} = \mathbb{F}_p(\mathrm{X})$ des fractions rationnelles sur $\mathbb{F}_p$ et notons π la projection $\mathbb{Z} \to \mathbb{F}_p$. D'une part, on a

$$(1 + \mathrm{X})^q = \sum_{i=0}^{q} \pi\left(\binom{q}{i}\right) \mathrm{X}^i. \tag{1}$$

D'autre part, comme $\mathrm{Fr}_q = \mathrm{Fr}_p^n$ est un endomorphisme de K, l'on a

$$(1 + \mathrm{X})^q = 1 + \mathrm{X}^q. \tag{2}$$

En comparant (1) et (2), on obtient que $\binom{q}{i} \equiv 0 \bmod p$, pour $i = 1, \ldots, q-1$. Ceci prouve le corollaire. □

Définition 15.22 **(Corps parfaits)**. — Soit k un corps. On dit que k est *parfait* si $\mathrm{car}(k) = 0$ ou bien si $\mathrm{car}(k) = p > 0$ et l'endomorphisme de Frobenius $k \to k$, $x \mapsto x^p$ est *surjectif*, et donc bijectif.

Exemple 15.23. — Tout corps fini est parfait. Par contre, le corps des fractions rationnelles $\mathbb{F}_p(\mathrm{T})$ n'est *pas* parfait, car T n'est pas une puissance p-ème (exercice : le démontrer !).

15.4. Éléments algébriques et polynômes minimaux. — Soit K/k une extension de corps et soit $\alpha \in \mathrm{K} \setminus \{0\}$. On renvoie au paragraphe 10.2 du Chapitre V pour la discussion de l'alternative « α algébrique ou transcendant ». Rappelons simplement les définitions et résultats suivants.

Définition 15.24. — On dit que α est **algébrique sur** k s'il existe un polynôme non nul $\mathrm{Q} \in k[\mathrm{X}]$ tel que $\mathrm{Q}(\alpha) = 0$.

Alors, l'idéal $\mathrm{I}_\alpha = \{\mathrm{Q} \in k[\mathrm{X}] \mid \mathrm{Q}(\alpha) = 0\}$ est un idéal *maximal*, engendré par un polynôme irréductible unitaire P uniquement déterminé, appelé le **polynôme minimal de** α **sur** k. C'est un polynôme **irréductible**, qu'on notera $\mathrm{Irr}_k(\alpha)$.

Son degré est noté $\deg_k(\alpha)$ et appelé le *degré de* α *sur* k. On remarque que

$$\alpha \in k \Leftrightarrow \deg_k(\alpha) = 1.$$

Proposition 15.25. — *On suppose* α *algébrique sur* k*, de degré* d*. Alors le sous-corps* $k(\alpha)$ *de* K *engendré par* α *est isomorphe au corps*

$$k[\mathrm{X}]/(\mathrm{Irr}_k(\alpha))$$

et admet pour base sur k *les monômes* $1, \ldots, \alpha^{d-1}$*. En particulier,* $k(\alpha)$ *coïncide avec* $k[\alpha]$*, la* sous-k-algèbre *de* K *engendrée par* α*, et l'on a :*

$$(\dagger) \qquad \dim_k k(\alpha) = d = \deg_k(\alpha).$$

Démonstration. — Voir le paragraphe 10.2. □

Remarquons que le polynôme minimal $\mathrm{Irr}_k(\alpha)$ dépend de α et de k. Plus précisément, on a la proposition suivante.

Proposition 15.26. — *Soient* $k \subseteq \mathrm{L} \subseteq \mathrm{K}$ *des corps (c.-à-d.,* L *est un* corps intermédiaire *de l'extension* K/k*). Si* $\alpha \in \mathrm{K}$ *est algébrique sur* k*, il l'est aussi sur* L *et le polynôme minimal* $\mathrm{Irr}_\mathrm{L}(\alpha)$ *divise* $\mathrm{Irr}_k(\alpha)$ *dans* $\mathrm{L}[\mathrm{X}]$*. En particulier, on a*

$$\deg_\mathrm{L}(\alpha) \leqslant \deg_k(\alpha).$$

Démonstration. — Posons $\mathrm{P} = \mathrm{Irr}_k(\alpha) \in k[\mathrm{X}]$. C'est un élément de $\mathrm{L}[\mathrm{X}]$ tel que $\mathrm{P}(\alpha) = 0$; par conséquent α est algébrique sur L et son polynôme minimal $\mathrm{Irr}_\mathrm{L}(\alpha)$ divise P dans $\mathrm{L}[\mathrm{X}]$. □

Définition 15.27 **(Extensions algébriques)**. — Soit K/k une extension de corps. On dit c'est une extension *algébrique* si tout élément de K est algébrique sur k.

Définition 15.28 **(Degré d'une extension)**. — Soit K/k une extension de corps. La dimension de K comme k-espace vectoriel s'appelle le *degré de* K *sur* k et se note $[\mathrm{K} : k]$; c'est un élément de $\mathbb{N}^* \cup \{+\infty\}$.

(La terminologie est inspirée de l'égalité (†), dans le cas où $\mathrm{K} = k(\alpha)$, avec α algébrique sur k.)

Enfin, rappelons le résultat suivant, appelé « multiplicativité des degrés » (cf. Proposition 10.14), ou aussi « Théorème de la base téléscopique ».

***Théorème 15.29* (Base téléscopique).** — *Soient* $k \subseteq \mathrm{K} \subseteq \mathrm{L}$ *des corps. Alors* $[\mathrm{L} : k] = [\mathrm{L} : \mathrm{K}]\,[\mathrm{K} : k]$.

Démonstration. — Voir la proposition 10.14 du Chap. V. □

15.5. Extensions de degré fini. —

Lemme 15.30. — *Toute extension* K/k *de degré fini* d *est algébrique et de type fini. De plus, pour tout* $x \in \mathrm{K}$, *on a* $\deg_k(x) \leqslant d$.

Démonstration. — Soit K/k une extension de degré fini et soit $(x_1, \ldots, x_n)$ une base de K sur k. Alors les x_i engendrent K comme k-espace vectoriel, donc *a fortiori* comme k-algèbre et comme surcorps de k. Donc l'extension K/k est de type fini.

Soit $x \in \mathrm{K}$ arbitraire. Comme $[\mathrm{K} : k] = d$, alors les $d+1$ monômes $1, x, \ldots, x^d$ vérifient une relation de dépendance linéaire non triviale ; donc x est algébrique sur k, de degré $\leqslant d$. □

Réciproquement, on a le théorème suivant.

Théorème 15.31. — *Soit* K/k *une extension de corps. Si* $\mathrm{K} = k(x_1, \ldots, x_n)$ *et si chaque* x_i *est* **algébrique** *sur* k *de degré* d_i, *alors* $\mathrm{K} = k[x_1, \ldots, x_n]$, *c.-à-d.,* K *est engendré comme* k-**algèbre** *par les* x_i, *et* K/k *est* **algébrique** *et* **de degré fini** *; plus précisément, on a*

$$[\mathrm{K} : k] \leqslant d_1 \cdots d_n.$$

Démonstration. — Montrons que $\mathrm{K} = k[x_1, \ldots, x_n]$ et $[\mathrm{K} : k] \leqslant d_1 \cdots d_n$ par récurrence sur n. Si $n = 1$, c'est le théorème 10.11. On peut donc supposer $n \geqslant 2$ et l'assertion établie pour $n - 1$. Posons $\mathrm{K}' = k(x_1, \ldots, x_{n-1})$. Alors $\mathrm{K} = \mathrm{K}'(x_n)$ et x_n est algébrique sur K′ de degré $\leqslant d_n$ et donc, par l'hypothèse de récurrence plus le cas $n = 1$ appliqué à K′, on obtient :

$$(*) \qquad \mathrm{K} = \mathrm{K}'(x_n) = \mathrm{K}'[x_n] = k[x_1, \ldots x_n],$$

et

$$[\mathrm{K} : k] = [\mathrm{K} : \mathrm{K}']\,[\mathrm{K}' : k] \leqslant d_n d_{n-1} \cdots d_1.$$

Ceci achève la récurrence. Donc K est de degré fini sur k, et donc tout élément de K est algébrique sur k, d'après le lemme précédent. Le théorème est démontré. □

Remarque 15.32. — Une autre démonstration du théorème 15.31 est la suivante. Soit $\phi : k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{K}$ le morphisme de k-algèbres défini par $\phi(\mathrm{X}_i) = x_i$, pour $i = 1, \ldots, n$; on a $\phi(\mathrm{P}) = \mathrm{P}(x_1, \ldots, x_n) \in \mathrm{K}$ pour tout $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. L'image de ϕ est $\mathrm{A} := k[x_1, \ldots, x_n]$, la sous-$k$-algèbre de K engendré par les x_i. Comme chaque monôme x_i^n est combinaison k-linéaire

des monômes x_i^r, avec $0 \leqslant r < d_i$, on en déduit que A est engendrée sur k par les monômes

$$x_1^{r_1} \cdots x_n^{r_n},$$

où $r_i < d_i$ pour tout i. Par conséquent, A est une k-algèbre de dimension finie $\leqslant d_1 \cdots d_n$. De plus, A est intègre, puisque contenue dans K. D'après le lemme 15.34 ci-dessous, A est un corps, et l'égalité $(*)$ en résulte. Donc $\mathrm{K} = \mathrm{A}$ est de dimension $\leqslant d_1 \cdots d_n$ sur k.

Corollaire 15.33. — *Une extension de corps $k \subset \mathrm{K}$ est de degré fini si et seulement si elle est algébrique et de type fini.*

Terminons ce paragraphe par le lemme suivant, qu'il est indispensable de connaître, ainsi que sa démonstration.

Lemme 15.34. — *Soient k un corps et* A *une k-algèbre intègre, de dimension finie sur k. Alors* A *est un corps.*

Démonstration. — Soit $a \in \mathrm{A} \setminus \{0\}$. Alors l'application de multiplication

$$\phi_a : \mathrm{A} \longrightarrow \mathrm{A}, \qquad x \mapsto ax$$

est k-linéaire et *injective* (puisque $a \neq 0$ et A intègre). Comme A est un k-espace vectoriel *de dimension finie*, ϕ_a est donc bijective. Par conséquent, il existe $x \in \mathrm{A}$ tel que $ax = 1$, ce qui montre que a est inversible. □

15.6. Corps de rupture d'un polynôme irréductible. — Voyons maintenant comment *construire* des extensions de corps. La première construction est la suivante.

Théorème 15.35 **(Corps de rupture d'un polynôme irréductible)**
Soient k un corps et $\mathrm{P} \in k[\mathrm{X}]$ un polynôme irréductible. *Alors $\mathrm{K} := k[\mathrm{X}]/(\mathrm{P})$ est un surcorps de k dans lequel* P *a au moins une racine, à savoir l'image x de* X. *On l'appelle le* **corps de rupture de** P **sur** k.

Le couple (K, x) vérifie la propriété universelle suivante : pour toute extension $k \subset \mathrm{L}$ telle que P *admette dans* L *une racine α, il existe un* **unique** *k-morphisme $\psi : \mathrm{K} \to \mathrm{L}$ tel que $\psi(x) = \alpha$; son image est le sous-corps $k[\alpha]$ de* L. *En particulier, ψ est un isomorphisme si $\mathrm{L} = k[\alpha]$.*

Démonstration. — Comme $k[\mathrm{X}]$ est principal et P irréductible, alors l'idéal (P) est maximal, donc K est un corps. Notant x l'image de X dans K, on a $\mathrm{P}(x) = 0$ et donc $x \in \mathrm{K}$ est bien une racine de P. Ceci prouve la première assertion.

Soit maintenant $k \subset \mathrm{L}$ une extension telle que P admette dans L une racine α. Alors $\mathrm{Irr}_k(\alpha)$, le polynôme minimal de α sur k, divise P, donc égale $\lambda \mathrm{P}$, avec $\lambda \in k^\times$, puisque P est irréductible. Par conséquent, le morphisme de k-algèbres $\phi : k[\mathrm{X}] \to \mathrm{L}$ défini par $\phi(\mathrm{X}) = \alpha$ induit un morphisme $\psi : \mathrm{K} \to \mathrm{L}$

tel que $\psi(x) = \alpha$. De plus, ce morphisme est unique, puisque $\mathrm{K} = k[x]$ est engendré comme k-algèbre par x. Ceci prouve le théorème. □

Exemple 15.36. — $\mathbb{R}[\mathrm{X}]/(\mathrm{X}^2+1) \cong \mathbb{C}$. Plus généralement, montrez que pour tout binôme $\mathrm{P} = \mathrm{X}^2 + b\mathrm{X} + c$ tel que $\Delta := b^2 - 4c$ soit < 0, le corps $\mathbb{R}[\mathrm{X}]/(\mathrm{P})$ est isomorphe à $\mathbb{C}$.

Remarque 15.37. — L'exercice ci-dessus montre que des polynômes différents peuvent avoir des corps de rupture isomorphes.

Définition 15.38. — Soit $\mathrm{P} \in k[\mathrm{X}]$ irréductible. Il est commode de dire qu'une extension K de k est *un corps de rupture de* P *sur* k si $\mathrm{K} \cong k[\mathrm{X}]/(\mathrm{P})$.

Proposition 15.39. — *Soit* $\mathrm{K} = k(\alpha)$ *une extension algébrique monogène et soient* $\mathrm{P} = \mathrm{Irr}_k(\alpha)$ *et* $d = \deg \mathrm{P} = \deg_k(\alpha)$. *Alors :*

1) K *est un corps de rupture de* P *sur* k.

2) *Pour toute extension* L/k, *le nombre de* k*-morphismes* $\mathrm{K} \to \mathrm{L}$ *est égal au nombre de racines de* P *dans* L. *Par conséquent, on a*

$$\#\,\mathrm{Hom}_{k\text{-}alg.}(\mathrm{K},\mathrm{L}) \leqslant \deg \mathrm{P},$$

avec égalité si et seulement si P *a* d *racines distinctes dans* L.

Démonstration. — D'après le théorème, il existe un (unique) isomorphisme de $k[\mathrm{X}]/(\mathrm{P})$ sur le sous-corps de K engendré par α, envoyant X sur α. Ceci prouve 1).

Pour tout k-morphisme $\phi : \mathrm{K} \to \mathrm{L}$, $\phi(\alpha)$ est une racine de P dans L. Réciproquement, comme $\mathrm{K} \cong k[\mathrm{X}]/(\mathrm{P})$, alors toute racine β de P dans L définit un morphisme de k-algèbres $\phi_\beta : \mathrm{K} \to \mathrm{L}$ tel que $\phi_\beta(\alpha) = \beta$, et évidemment ces morphismes sont deux à deux distincts. Ceci prouve 2). □

Exemple 15.40. — Soient $k = \mathbb{Q}$ et $\mathrm{P} = \mathrm{X}^3 - 2$. Alors P est irréductible sur $\mathbb{Q}$, car il n'a pas de racine dans $\mathbb{Q}$. Notons $\sqrt[3]{2}$ la racine cubique réelle de 2 et $j = \exp(2i\pi/3)$, $j^2 = \exp(4i\pi/3)$ les racines primitives de l'unité d'ordre 3 dans $\mathbb{C}$. Les racines de P dans $\mathbb{C}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ et chacun des sous-corps suivants de $\mathbb{C}$:

$$\mathbb{Q}[\sqrt[3]{2}], \quad \mathbb{Q}[j\sqrt[3]{2}], \quad \mathbb{Q}[j^2\sqrt[3]{2}]$$

est un corps de rupture de P. Bien que $\mathbb{Q}$-isomorphes, ces trois sous-corps de $\mathbb{C}$ sont deux à deux distincts. En effet, $\mathbb{Q}[\sqrt[3]{2}]$ est contenu dans $\mathbb{R}$, donc distinct des deux autres. Si l'on avait $\mathbb{Q}[j\sqrt[3]{2}] = \mathbb{Q}[j^2\sqrt[3]{2}]$, alors ce corps, disons K, contiendrait j et donc $\sqrt[3]{2}$, donc contiendrait $\mathbb{Q}[\sqrt[3]{2}]$. Comme ces deux corps sont de même dimension $\deg \mathrm{P} = 3$ sur $\mathbb{Q}$, on aurait $\mathbb{Q}[\sqrt[3]{2}] = \mathrm{K}$, ce qui n'est pas le cas.

15.7. Corps de décomposition d'un polynôme. —

Définition 15.41. — Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme non constant. On dit qu'une extension K de k est un **corps de décomposition de** P **sur** k si elle vérifie les deux conditions suivantes :

1) P a toutes ses racines dans K, c.-à-d., est scindé dans K[X].

2) K est engendré sur k par les racines de P. (Ceci entraîne que K est de degré fini sur k, d'après le théorème 15.31.)

Théorème 15.42 **(Corps de décomposition d'un polynôme)**
Tout $\mathrm{P} \in k[\mathrm{X}]$ *non constant admet un corps de décomposition sur* k*, unique à* k*-isomorphisme près.*

Démonstration. — On va démontrer **l'existence** d'un corps de décomposition de P sur k par récurrence sur $n = \deg \mathrm{P}$. Si $n = 1$, alors $\mathrm{P} = a\mathrm{X} - b = a(\mathrm{X} - b/a)$ et k est un corps de décomposition de P. Supposons $n \geqslant 2$ et le théorème établi pour tout corps et tout polynôme de degré $< n$, et soit $\mathrm{P} \in k[\mathrm{X}]$ de degré n.

Soit S un facteur irréductible de P et soit $k_1 = k(\alpha)$ un corps de rupture de S. Alors, dans $k_1[\mathrm{X}]$, on a $\mathrm{P} = (\mathrm{X} - \alpha)\mathrm{Q}$, avec $\mathrm{Q} \in k_1[\mathrm{X}]$ de degré $n - 1$. Par hypothèse de récurrence, il existe une extension K/k_1 dans laquelle Q a des racines $\alpha_2, \ldots, \alpha_n$ et telle que $\mathrm{K} = k_1(\alpha_2, \ldots, \alpha_n)$. Alors, $\alpha, \alpha_2, \ldots, \alpha_n$ sont les racines de P dans K, et K est engendré sur k par ces élements. Ceci montre l'existence d'un corps de décomposition.

Pour montrer l'unicité à isomorphisme près, on va procéder par récurrence (sur le nombre m de racines de P qui sont dans K mais pas dans k). Pour les besoins de cette démonstration par récurrence, il est nécessaire de formuler et démontrer le théorème d'unicité sous la forme du théorème 15.44 ci-dessous (le cas particulier $k = k'$ et $\tau = \mathrm{id}_k$ fournit l'unicité à k-isomorphisme près du corps de décomposition).

Commençons par le lemme ci-dessous.

Lemme 15.43. — *Soit* $\tau : k \xrightarrow{\sim} k'$ *un isomorphisme de corps. Il induit un isomorphisme d'anneaux*

$$\phi_\tau : k[\mathrm{X}] \xrightarrow{\sim} k'[\mathrm{X}], \qquad \sum_i a_i \mathrm{X}^i \mapsto \sum_i \tau(a_i)\mathrm{X}^i.$$

De plus, pour tout $\mathrm{P} \in k[\mathrm{X}]$, ϕ_τ *induit un isomorphisme d'anneaux*

$$k[\mathrm{X}]/(\mathrm{P}) \xrightarrow{\sim} k'[\mathrm{X}]/(\tau(\mathrm{P})).$$

Démonstration. — L'isomorphisme $\tau : k \xrightarrow{\sim} k'$ munit k', et donc aussi $k'[\mathrm{X}]$, d'une structure de k-algèbre. D'après la propriété universelle de $k[\mathrm{X}]$, il existe

un unique morphisme de k-algèbres $\phi_\tau : k[\mathrm{X}] \to k'[\mathrm{X}]$ tel que $\phi_\tau(\mathrm{X}) = \mathrm{X}$, et ϕ_τ vérifie la formule donnée ci-dessus.

On obtient de même que l'isomorphisme $\tau^{-1} : k' \xrightarrow{\sim} k$ induit un morphisme

$$\phi_{\tau^{-1}} : k'[\mathrm{X}] \xrightarrow{\sim} k[\mathrm{X}], \qquad \sum_i a_i \mathrm{X}^i \mapsto \sum_i \tau^{-1}(a_i)\mathrm{X}^i,$$

et il est alors clair que ϕ_τ et $\phi_{\tau^{-1}}$ sont inverses l'un de l'autre. Ceci prouve la première assertion.

Enfin, pour tout $\mathrm{P} \in k[\mathrm{X}]$, il est clair que ϕ_τ et $\phi_{\tau^{-1}}$ induisent des bijections réciproques entre les idéaux (P) et $(\tau(\mathrm{P}))$, et donc entre les anneaux quotients $k[\mathrm{X}]/(\mathrm{P})$ et $k'[\mathrm{X}]/(\tau(\mathrm{P}))$. Ceci prouve le lemme. □

***Théorème 15.44* (Unicité du corps de décomposition).** — *Soient $\tau : k \xrightarrow{\sim} k'$ un isomorphisme de corps, $\mathrm{P} \in k[\mathrm{X}]$ non constant et K, resp. K', un corps de décomposition de P sur k, resp. de $\tau(\mathrm{P})$ sur k'. Alors τ se prolonge en un isomorphisme $\sigma : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$.*

Démonstration. — On procède par récurrence sur le **nombre m de racines de P qui sont dans K mais pas dans k**. Sans perte de généralité, on peut supposer P unitaire. Si $m = 0$, alors

$$\mathrm{P} = (\mathrm{X} - \lambda_1) \cdots (\mathrm{X} - \lambda_n),$$

avec les λ_i dans k. Dans ce cas, $\mathrm{K} = k$ et

$$\tau(\mathrm{P}) = (\mathrm{X} - \tau(\lambda_1)) \cdots (\mathrm{X} - \tau(\lambda_n)),$$

avec $\tau(\lambda_i) \in k'$, donc $\mathrm{K}' = k'$ et l'on peut prendre $\sigma = \tau$.

Supposons $m > 0$ et le théorème établi pour tout $m' < m$. Soit $\mathrm{P} \in k[\mathrm{X}]$ ayant exactement m racines dans $\mathrm{K} \setminus k$, et soit

$$\mathrm{P} = \mathrm{P}_1 \cdots \mathrm{P}_r \tag{1}$$

sa décomposition en facteurs irréductibles dans $k[\mathrm{X}]$. Comme $m > 0$, l'un au moins de ces facteurs, disons P_1, est de degré $\geqslant 2$ et n'a pas de racines dans k.

Par hypothèse, P se scinde dans $\mathrm{K}[\mathrm{X}]$ comme produit de facteurs (irréductibles !) de degré 1. Comme $\mathrm{K}[\mathrm{X}]$ est **factoriel**, l'unicité d'une telle décomposition entraîne que chaque P_i est un produit de certains de ces facteurs linéaires. En particulier, P_1 a toutes ses racines dans K. Soit α l'une d'elles. D'après la proposition 15.39, on a un k-isomorphisme

$$\psi : k[\mathrm{X}]/(\mathrm{P}_1) \xrightarrow{\sim} k[\alpha]. \tag{2}$$

D'autre part,

$$\tau(\mathrm{P}) = \tau(\mathrm{P}_1) \cdots \tau(\mathrm{P}_r), \tag{1'}$$

et, par le même argument que précédemment, chaque $\tau(\mathrm{P}_i)$ a toutes ses racines dans K'. Soit β une racine de $\tau(\mathrm{P}_1)$ dans K'. D'après la proposition 15.39, à nouveau, on a un k'-isomorphisme

$$\psi' : k'[\mathrm{X}]/(\tau(\mathrm{P}_1)) \xrightarrow{\sim} k'[\beta]. \tag{2'}$$

De plus, d'après le lemme 15.43, on a un isomorphisme

$$\phi_\tau : k[\mathrm{X}]/(\mathrm{P}_1) \xrightarrow{\sim} k'[\mathrm{X}]/(\tau(\mathrm{P}_1))$$

qui prolonge $\tau : k \xrightarrow{\sim} k'$. Posons $k_1 = k[\alpha]$ et $k'_1 = k'[\beta]$. Alors, $\tau_1 := \psi' \circ \phi_\tau \circ \psi^{-1}$ est un isomorphisme $k_1 \xrightarrow{\sim} k'_1$ qui prolonge τ. On a donc le diagramme suivant :

$$\begin{array}{ccccc} k & \subset & k_1 & \subset & \mathrm{K} \\ \tau\downarrow & \cong & \tau_1\downarrow & \cong & \\ k' & \subset & k'_1 & \subset & \mathrm{K}'. \end{array}$$

Maintenant, K (resp. K') est un corps de décomposition sur k_1 (resp. sur k'_1) de notre polynôme P (resp. de $\tau(\mathrm{P})$), et le nombre de racines de P dans $\mathrm{K} \setminus k_1$ est $< m$. Donc, par hypothèse de récurrence, il existe un isomorphisme $\sigma : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$ tel que $\sigma|_{k_1} = \tau_1$. Par conséquent, $\sigma|_k = \tau_1|_k = \tau$. Ceci prouve le théorème 15.44 et achève la preuve du théorème 15.42. □

□

Remarque 15.45. — Voici une **autre démonstration** des deux théorèmes précédents, qui utilise l'existence d'une clôture algébrique de k, et d'autres résultats prouvés dans le paragraphe suivant. (Ces résultats n'utilisent pas la notion de corps de décomposition, donc il n'y a pas de cercle vicieux dans l'argument.)

Soit Ω une clôture algébrique de k, soient $\alpha_1, \ldots, \alpha_n$ les racines de P dans Ω et soit K_0 le sous-corps de Ω engendré par les α_i. Il est clair que K_0 est un corps de décomposition de P sur k. Ceci prouve l'existence.

Démontrons maintenant l'unicité, sous la forme plus forte donnée dans le théorème 15.44.

Posons $\mathrm{P}' = \tau(\mathrm{P})$ et soient $\beta_1, \ldots, \beta_n$ les racines de P' dans K'. Soit Ω une clôture algébrique de k. Traitons d'abord le cas où $\mathrm{K} = \mathrm{K}_0$ est le sous-corps de Ω engendré par les racines $\alpha_1, \ldots, \alpha_n$ de P de Ω.

Comme l'extension $k \xrightarrow{\sim} k' \subseteq \mathrm{K}'$ est algébrique alors, d'après le théorème 15.54, l'injection $k \hookrightarrow \Omega$ se prolonge en une injection

$$\phi : \mathrm{K}' \hookrightarrow \Omega,$$

telle que $\phi(\mathrm{P}') = \phi(\tau(\mathrm{P})) = \mathrm{P}$. Par conséquent, les racines β_i de P' dans K' sont envoyées par ϕ sur les racines de P dans Ω, et comme K' est engendré sur k' par les β_i, alors $\phi(\mathrm{K}')$ est engendré sur $\phi(k') = k$ par les α_i, et donc $\phi(\mathrm{K}') = \mathrm{K}_0$. Ceci prouve le résultat voulu pour $\mathrm{K} = \mathrm{K}_0$.

Enfin, pour K arbitraire, le même raisonnement fournit un k-isomorphisme $\psi : \mathrm{K} \xrightarrow{\sim} \mathrm{K}_0$. Alors,

$$\phi^{-1} \circ \psi : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$$

est un isomorphisme prolongeant τ.

15.8. Extensions algébriques et clôtures algébriques. —

***Théorème 15.46* (Transitivité des extensions algébriques)**
Soient $k \subseteq \mathrm{K} \subseteq \mathrm{L}$ des corps. On suppose l'extension K/k algébrique. Alors, tout $x \in \mathrm{L}$ qui est algébrique sur K l'est aussi sur k.

En particulier, si l'extension L/K est algébrique, alors L/k l'est aussi.

Démonstration. — Soit $x \in \mathrm{L}$, algébrique sur K. Il existe donc $n \in \mathbb{N}^*$ et $a_0, \ldots, a_{n-1} \in \mathrm{K}$ tels que

$$(*) \qquad x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Par hypothèse, chaque a_i est algébrique sur k ; donc, d'après le théorème 15.31, le sous-corps

$$k' := k(a_0, \ldots, a_{n-1})$$

de K est de **degré fini** sur k. De plus, $(*)$ montre que x est algébrique sur k', donc l'extension $k' \subseteq k'(x)$ est aussi de degré fini $\deg_{k'}(x)$. D'où, par multiplicativité des degrés,

$$[k'(x) : k] = \deg_{k'}(x)\,[k' : k] < \infty.$$

Par conséquent, d'après le lemme 15.30, x est algébrique sur k. Ceci prouve le théorème. □

Définition 15.47. — Soit $k \subseteq \mathrm{K}$ une extension de corps. On dit que K est une **clôture algébrique de** k s'il vérifie les deux conditions suivantes :

a) K est algébriquement clos ;

b) K est **algébrique sur** k, c.-à-d., tout élément de K est algébrique sur k.

Remarque 15.48. — On a vu (Chap. V, Théorème 10.24) que $\mathbb{C}$ est algébriquement clos. Mais **attention**, $\mathbb{C}$ n'est **pas** algébrique sur $\mathbb{Q}$ car $\mathbb{C}$ contient des éléments qui ne sont pas algébriques sur $\mathbb{Q}$, par exemple $\pi = 3,1415926\ldots$ ou $e = 2,7182818\ldots$.

***Théorème 15.49* (Steinitz)**. — *Tout corps k admet une clôture algébrique, unique à k-isomorphisme (non-unique) près.*

Avant de démontrer ce théorème, établissons la proposition et le corollaire qui suivent.

Proposition 15.50 **(Fermeture algébrique de k dans K).** — *Soit K/k une extension de corps.*

1) *Le sous-ensemble*

$$\mathrm{K}_{\mathrm{alg}/k} = \{x \in \mathrm{K} \mid x \text{ est algébrique sur } k\}$$

est un sous-corps de K, appelé la fermeture algébrique de k dans K.

2) *Tout $x \in \mathrm{K}$ qui est algébrique sur $\mathrm{K}_{\mathrm{alg}/k}$ appartient à $\mathrm{K}_{\mathrm{alg}/k}$ et donc $\mathrm{K}_{\mathrm{alg}/k}$ est égal à sa fermeture algébrique dans K.*

En particulier, si K est algébriquement clos alors $\mathrm{K}_{\mathrm{alg}/k}$ est une clôture algébrique de k.

Démonstration. — Posons $\mathrm{K}' = \mathrm{K}_{\mathrm{alg}/k}$. Il est clair que $1 \in \mathrm{K}'$. Soient $x, y \in \mathrm{K}'$. Alors la sous-algèbre $k[x]$ est un corps, de degré $d = \deg_k(x)$ sur k. Comme y est algébrique sur k, il l'est aussi sur $k[x]$ et donc la sous-algèbre $k[x,y] = k[x][y]$ est un corps, égal à $k(x,y)$, et de degré $f = \deg_{k[x]}(y)$ sur $k[x]$. Donc,

$$[k(x,y) : k] = [k(x,y) : k(x)]\,[k(x) : k] = fd < \infty.$$

Comme $k(x,y)$ contient $x+y$ et xy, ces deux éléments sont algébriques sur k, c.-à-d., appartiennent à K'. Ceci montre que K' est un sous-corps de K, ce qui prouve 1).

2) Soit $x \in \mathrm{K}$ algébrique sur K'. D'après le théorème 15.46, x est algébrique sur k, donc $x \in \mathrm{K}'$. Ceci prouve la première assertion.

Supposons de plus K algébriquement clos, et montrons que K' est une clôture algébrique de k. Par définition, K' est algébrique sur k, donc il suffit de montrer qu'il est algébriquement clos.

Soit $\mathrm{P} = a_0 + a_1\mathrm{X} + \cdots + a_d\mathrm{X}^d \in \mathrm{K}'[\mathrm{X}]$, non constant. Comme K est algébriquement clos, il existe $\alpha \in \mathrm{K}$ tel que $\mathrm{P}(\alpha) = 0$. Alors α est algébrique sur K', donc appartient à K'. Ceci montre que K' est algébriquement clos. La proposition est démontrée. □

Comme $\mathbb{C}$ est algébriquement clos, on obtient ainsi le corollaire suivant.

Corollaire 15.51. — *Le corps $\overline{\mathbb{Q}} := \{z \in \mathbb{C} \mid z \text{ est algébrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$.*

Démontrons maintenant le théorème de Steinitz. Désignons par

$$\{\mathrm{P}_\lambda \mid \lambda \in \Lambda\}$$

l'ensemble des polynômes irréductibles unitaires de $k[\mathrm{X}]$, et soit A la k-algèbre de polynômes en une infinité de variables X_λ, pour $\lambda \in \Lambda$. Pour tout $\lambda \in \Lambda$, soit

$$\mathrm{P}_\lambda(\mathrm{X}_\lambda)$$

l'image de P_λ dans A par le morphisme $k[\mathrm{X}] \to \mathrm{A}$ qui envoie X sur X_λ ; c.-à-d.,

$$\text{si } \ \mathrm{P}_\lambda = \mathrm{X}^d + \sum_{i=1}^{d} a_i \, \mathrm{X}^i, \qquad \text{alors } \ \mathrm{P}_\lambda(\mathrm{X}_\lambda) = \mathrm{X}_\lambda^d + \sum_{i=1}^{d} a_i \, \mathrm{X}_\lambda^i.$$

Notons I l'idéal de A engendré par les éléments $\mathrm{P}_\lambda(\mathrm{X}_\lambda)$, pour $\lambda \in \Lambda$.

Lemme 15.52. — I *est un idéal propre de* A.

Démonstration. — En effet, sinon il existerait un sous-ensemble fini $\Lambda_0 = \{\lambda_1, \ldots, \lambda_n\}$ de Λ tel que

$$(*) \qquad 1 = \sum_{i=1}^{n} \mathrm{Q}_i \mathrm{P}_{\lambda_i}(\mathrm{X}_{\lambda_i}),$$

avec $\mathrm{Q}_i \in \mathrm{A}$. Désignons par Λ_1 la réunion de Λ_0 et des variables X_λ qui apparaissent dans $\mathrm{Q}_1, \ldots, \mathrm{Q}_n$; c'est un ensemble fini

$$\Lambda_1 = \{\lambda_1, \ldots, \lambda_n, \lambda_{n+1}, \ldots, \lambda_{\mathrm{N}}\},$$

et l'égalité $(*)$ a lieu dans l'anneau de polynômes $\mathrm{B} := k[\mathrm{X}_{\lambda_j} \mid j = 1, \ldots, \mathrm{N}]$, en un nombre fini de variables.

Soit k_1 un corps de rupture sur k du polynôme irréductible P_{λ_1} et soit α_1 une racine dans k_1 de P_{λ_1}.

Le polynôme P_{λ_2} n'est pas nécessairement irréductible sur k_1, mais peu importe : soit P_2 un facteur irréductible de P_{λ_2} dans $k_1[\mathrm{X}]$ et soit k_2 un corps de rupture sur k_1 de P_2. Alors

$$k \subset k_1 \subseteq k_2$$

et P_{λ_1} et P_{λ_2} ont une racine α_1, resp. α_2, dans k_2. Répétant ce processus, on obtient un surcorps $\mathrm{K} = k_n$ de k dans lequel chaque P_{λ_i} a une racine α_i, pour $i = 1, \ldots, n$. Alors, l'égalité $(*)$ a lieu dans l'anneau de polynômes

$$\mathrm{B}_\mathrm{K} := \mathrm{K}[\mathrm{X}_{\lambda_j} \mid j = 1, \ldots, \mathrm{N}],$$

et on peut considérer le morphisme

$$\phi : \mathrm{B} \longrightarrow \mathrm{K}$$

défini par $\phi(\mathrm{X}_{\lambda_i}) = \alpha_i$, pour $i = 1, \ldots, n$ et $\phi(\mathrm{X}_j) = 0$ pour $j = n+1, \ldots, \mathrm{N}$, c.-à-d.,

$$\forall \, \mathrm{Q} \in \mathrm{B}_\mathrm{K}, \qquad \phi(\mathrm{Q}) = \mathrm{Q}(\alpha_1, \ldots, \alpha_n, 0, \ldots, 0).$$

Alors, appliquant ϕ à l'égalité $(*)$, on obtient $1 = 0$, une contradiction. Cette contradiction montre que I est un idéal propre de A. Le lemme est démontré. □

Donc, puisque I est un idéal propre de A, il est contenu dans un idéal maximal $\mathfrak{m}$. Posons $\mathrm{K}_1 = \mathrm{A}/\mathfrak{m}$ et $\mathrm{K}_0 = k$. Pour tout $\lambda \in \Lambda$, notons x_λ l'image de X_λ dans K_1 ; c'est une racine du polynôme P_λ.

Proposition 15.53. — 1) *Tout polynôme irréductible de* $k[\mathrm{X}]$ *a une racine dans* K_1.

2) *De plus,* K_1 *est algébrique sur* $k = \mathrm{K}_0$.

Démonstration. — 1) est immédiat, car les polynômes irréductibles unitaires de $k[\mathrm{X}]$ sont les P_λ, et chacun a une racine x_λ dans K_1.

2) Soit $y \in \mathrm{K}_1$. Alors y est l'image dans K_1 d'un polynôme $\mathrm{Q} \in \mathrm{A}$ qui, nécessairement, ne fait intervenir qu'un nombre fini de variables X_{λ_i}, pour $i = 1, \ldots, s$. Donc y appartient à la sous-algèbre

$$\mathrm{C} := k[x_{\lambda_1}, \ldots, x_{\lambda_s}]$$

de K_1, et comme chaque x_{λ_i} est algébrique sur k (puisque racine du polynôme P_{λ_i}), on a, d'après le théorème 15.31, $\dim_k \mathrm{C} < \infty$ et donc y est algébrique sur $k = \mathrm{K}_0$. La proposition est démontrée. □

Si K_1 n'est pas algébriquement clos, on peut appliquer à K_1 le même processus : on obtient ainsi une extension algébrique $\mathrm{K}_1 \subseteq \mathrm{K}_2$ dans laquelle tout polynôme irréductible de $\mathrm{K}_1[\mathrm{X}]$ a au moins une racine ; de plus, par transitivité (théorème 15.46), l'extension $\mathrm{K}_2/\mathrm{K}_0$ est algébrique. On construit ainsi une suite croissante d'extensions algébriques :

$$k = \mathrm{K}_0 \subseteq \mathrm{K}_1 \subseteq \mathrm{K}_2 \subseteq \cdots$$

telle que tout polynôme irréductible $\mathrm{P} \in \mathrm{K}_i[\mathrm{X}]$ a une racine dans K_{i+1}. Alors

$$\mathrm{K} = \bigcup_{i \geqslant 0} \mathrm{K}_i$$

est un corps, algébrique sur $k = \mathrm{K}_0$, et algébriquement clos. En effet, tout polynôme irréductible $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ a tous ses coefficients dans un certain K_i, donc a une racine dans K_{i+1}, donc dans K. Ceci montre que k admet une clôture algébrique. (Cette démonstration est dûe à Emil Artin.)

Il reste à montrer l'unicité, à isomorphisme près.

Théorème 15.54. — *Soient* K/k *une extension algébrique,* Ω *un corps algébriquement clos, et* $\tau : k \hookrightarrow \Omega$ *un morphisme de corps. Alors* τ *se prolonge à* K *(de façon non unique en général).*

Démonstration. — Soit E l'ensemble des couples (k', τ') où k'/k est une sous-extension de K/k et où τ' est un morphisme $k' \to \Omega$ prolongeant τ. Alors E

est non vide, car il contient le couple (k, τ). On munit E de la relation d'ordre définie par :

$$(k', \tau') \leqslant (k'', \tau'') \Leftrightarrow k' \subseteq k'' \quad \text{et } \tau'' \text{ prolonge } \tau'.$$

Alors E est un ensemble ordonné **inductif**, c.-à-d., tout sous-ensemble filtrant admet un majorant dans E. En effet, si $(k_i, \tau_i)_{i\in \mathrm{I}}$ est une famille filtrante d'élements de E, alors

$$k' = \bigcup_{i\in \mathrm{I}} k_i$$

est un sous-corps de K, et les τ_i se prolongent en un morphisme $\tau' : k' \to \Omega$ défini par $\tau'(x) = \tau_i(x)$ si $x \in k_i$. Ceci est bien défini, car si $x \in k_j$ avec $j \neq i$, il existe $\ell \in \mathrm{I}$ tel que k_ℓ contienne k_i et k_j et alors

$$\tau_i(x) = \tau_\ell(x) = \tau_j(x).$$

Ceci montre que E est bien inductif, c.-à-d., vérifie l'hypothèse du théorème de Zorn (Théorème 12.7, Chap. VI). Donc, d'après le théorème de Zorn, E possède (au moins) un élément maximal (k_0, τ_0).

Montrons que $k_0 = \mathrm{K}$. Soit $x \in \mathrm{K}$. Alors x est algébrique sur k donc *a fortiori* sur k_0. Soit $\mathrm{P} \in k_0[\mathrm{X}]$ son polynôme minimal sur k_0. Alors le polynôme $\tau_0(\mathrm{P})$ a une racine α dans Ω, puisque Ω est algébriquement clos. Identifiant k_0 à son image dans Ω par τ_0, on obtient des isomorphismes

$$k_0[\alpha] \cong k_0[\mathrm{X}]/(\mathrm{P}) \cong k_0[x].$$

Par conséquent, τ_0 se prolonge en un morphisme

$$k_0[x] \xrightarrow{\sim} k_0[\alpha] \hookrightarrow \Omega.$$

Par maximalité de (k_0, τ_0), ceci entraîne $k_0 = k_0[x]$, d'où $x \in k_0$. Ceci montre que $k_0 = \mathrm{K}$, et donc τ se prolonge en $\tau_0 : \mathrm{K} \to \Omega$. Ceci prouve le théorème 15.54. □

Le dernier ingrédient pour achever la preuve du théorème de Steinitz est le résultat suivant, qui est intéressant en lui-même.

Lemme 15.55. — *Soit* L *une clôture algébrique de* k. *Alors* $k \subseteq \mathrm{L}$ *est une* **extension algébrique maximale**, *c.-à-d., si on a une extension*

$$k \subseteq \mathrm{L} \subseteq \mathrm{L}' \qquad \textit{avec } \mathrm{L}' \textit{ algébrique sur } k,$$

alors $\mathrm{L}' = \mathrm{L}$.

Démonstration. — Soit $x \in \mathrm{L}'$. Alors x est algébrique sur k donc *a fortiori* sur L. Soit P son polynôme minimal sur L. Comme L est algébriquement clos, P est de degré 1, c.-à-d., $x \in \mathrm{L}$. □

Corollaire 15.56. — *Soient* Ω, Ω' *deux clôtures algébriques de* k. *Alors il existe un* k*-isomorphisme* $\phi : \Omega \xrightarrow{\sim} \Omega'$.

Démonstration. — D'après le théorème 15.54 appliqué à $\mathrm{K} = \Omega'$, l'injection $\tau : k \hookrightarrow \Omega$ se prolonge en une injection

$$k \hookrightarrow \Omega' \overset{\tau'}{\hookrightarrow} \Omega.$$

Alors, comme Ω' est algébriquement clos et Ω/k algébrique, l'injection τ' est surjective, c.-à-d., c'est un k-isomorphisme $\Omega' \xrightarrow{\sim} \Omega$. Ceci prouve le corollaire et achève la preuve du théorème de Steinitz 15.49. □

15.9. Bases de transcendance. — [(8)] Afin de couvrir les extensions de type fini K/k arbitraires (c.-à-d., pas nécessairement algébriques), traitons dans ce paragraphe la notion de base (et degré) de transcendance

Soit K/k une extension de corps, et soient $x_1, \ldots, x_n \in \mathrm{K}$.

Définition 15.57. — On dit que $x_1, \ldots, x_n$ sont **algébriquement indépendants sur** k si le morphisme

$$\phi : k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \longrightarrow \mathrm{K}, \qquad \mathrm{P} \mapsto \mathrm{P}(x_1, \ldots, x_n)$$

est injectif. Dans ce cas, ϕ se prolonge en un isomorphisme de $k(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ sur le sous-corps de K engendré par les x_i. En particulier, chaque x_i est transcendant sur k.

Remarque 15.58. — Soit K le corps des fractions de l'anneau $k[x, y]$, où $x^2 = y^3$. Alors x et y sont transcendants sur k, mais ne sont pas algébriquement indépendants sur k, puisqu'on a la relation $x^2 = y^3$.

Définition 15.59. — On dit qu'une partie B de K est une **base de transcendance sur** k si elle vérifie les deux conditions suivantes :

(i) les éléments de B sont algébriquement indépendants sur k ;

(ii) le corps K est extension algébrique du sous-corps $k(\mathrm{B})$.

Ceci équivaut à dire que B est une partie **algébriquement indépendante maximale**.

Lemme 15.60. — *Soit* K/k *une extension et soit* S *une partie* **finie** *de* K *telle que* K *soit algébrique sur* $k(\mathrm{S})$. *Alors* S *contient une base de transcendance* B *de* K *sur* k. *De plus,* $[k(\mathrm{S}) : k(\mathrm{B})] < \infty$ *; en particulier, si* $\mathrm{K} = k(\mathrm{S})$, *alors* K *est de degré fini sur* $k(\mathrm{B})$.

Démonstration. — Posons $\mathrm{S} = \{x_1, \ldots, x_n\}$. Quitte à renuméroter les x_i, on peut supposer que $x_1, \ldots, x_r$ sont algébriquement indépendants sur k et que, pour tout $i > r$, x_i est algébrique sur $k(\mathrm{B})$, où $\mathrm{B} = \{x_1, \ldots, x_r\}$. Alors, par transitivité des extensions algébriques (15.46), K est algébrique sur $k(\mathrm{B})$, et donc B est une base de transcendance de K sur k.

[(8)] Ce paragraphe n'a pas été traité en cours.

De plus, d'après le théorème 15.31, $k(\mathrm{S})$ est de degré fini sur $k(\mathrm{B})$. □

Proposition 15.61. — *Soit* K/k *une extension de corps telle que* K *possède une base de transcendance sur* k **finie**.

1) *Soit* B *une base de transcendance de* K *sur* k *de cardinal* **minimum** n. *Alors, toute partie* B' *algébriquement indépendante sur* k *est de cardinal* $\leqslant n$.

2) *Par conséquent,* **toute** *base de transcendance de* K *sur* k *est de cardinal* n.

Démonstration. — On procède par récurrence sur l'entier $s(\mathrm{B}, \mathrm{B}') := \#\mathrm{B} - \#(\mathrm{B} \cap \mathrm{B}')$. Si $s = 0$, alors $\mathrm{B} \subseteq \mathrm{B}'$ donc $\mathrm{B}' = \mathrm{B}$ par maximalité de B. On peut donc supposer $s \geqslant 1$ et l'assertion établie pour $s - 1$.

Écrivons $\mathrm{B} = \{b_1, \ldots, b_n\}$. Sans perte de généralité, on peut supposer que

$$\mathrm{B} \cap \mathrm{B}' = \{b_{s+1}, \ldots, b_n\}.$$

Si $\mathrm{B}' \subseteq \mathrm{B}$, l'assertion est vérifiée, donc on peut supposer qu'il existe $b' \in \mathrm{B}'$ tel que $b' \notin \mathrm{B}$. Alors $\mathrm{B} \cup \{b'\}$ n'est pas algébriquement indépendante, par maximalité de B. Donc, il existe $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n, \mathrm{X}_{n+1}]$ non nul tel que

$$\mathrm{P}(b_1, \ldots, b_n, b') = 0.$$

De plus, $\mathrm{P} \notin k[\mathrm{X}_{s+1}, \ldots, \mathrm{X}_{n+1}]$, puisque les éléments de B' sont algébriquement indépendants. Donc, sans perte de généralité, on peut supposer que P contient la variable X_1.

Posons alors $\mathrm{B}_1 = \{b_2, \ldots, b_n, b'\}$. Alors b_1 est algébrique sur $k(\mathrm{B}_1)$, et comme K est algébrique sur $k(\mathrm{B}_1)[b_1]$, il est aussi algébrique sur $k(\mathrm{B}_1)$.

Comme $\#\mathrm{B}_1 = n$, la minimalité de n, jointe au lemme 15.60, entraîne que B_1 est une base de transcendance de K sur k (car sinon, B_1 contiendrait une base de transcendance de K sur k de cardinal $< n$, contredisant la minimalité de n). De plus,

$$\#\mathrm{B}_1 - \#(\mathrm{B}_1 \cap \mathrm{B}') = s - 1, \quad \text{car} \quad \mathrm{B}_1 \cap \mathrm{B}' = \{b_{s+1}, \ldots, b_n, b'\}.$$

Donc, par l'hypothèse de récurrence, appliquée à B_1 et B', on obtient que $\#\mathrm{B}' \leqslant \#\mathrm{B}_1 = n$. Ceci prouve 1).

En particulier, si B' est une autre base de transcendance de K/k, alors $\#\mathrm{B}' \leqslant n$, et donc $\#\mathrm{B}' = n$ par minimalité de n. La proposition est démontrée. □

Théorème 15.62. — *Soit* $k \subset \mathrm{K}$ *une extension de corps de type fini. Alors :*

1) *Toutes les bases de transcendance de* K *ont le même cardinal, appelé* **degré de transcendance de** K **sur** k *et noté* $\deg \mathrm{tr}_k \mathrm{K}$. *De plus, tout ensemble d'éléments algébriquement indépendants est contenu dans une base de transcendance.*

2) *Soit* L/k *une sous-extension de* K/k (*c.-à-d.,* L *est un sous-corps de* K *contenant* k). *Alors* L/k *est de type fini et l'on a*

$$\deg \mathrm{tr}_k \mathrm{L} \leqslant \deg \mathrm{tr}_k \mathrm{K}.$$

Démonstration. — D'après le lemme 15.60, il existe une base de transcendance B_0 de K sur k ayant r éléments. Alors, d'après la proposition précédente, toute base de transcendance de K sur k a r éléments, et toute partie algébriquement libre est de cardinal $\leqslant r$. Par conséquent, toute suite croissante de parties algébriquement indépendantes est stationnaire (après au plus r étapes), et donc toute partie algébriquement indépendante est contenue dans une partie algébriquement indépendante maximale, c.-à-d., dans une base de transcendance de K sur k. Ceci prouve 1).

Démontrons 2). Comme toute partie de L algébriquement indépendante sur k est aussi une partie de K algébriquement indépendante sur k, on obtient que L possède une base de transcendance finie $\mathrm{B} = \{b_1, \ldots, b_t\}$, qu'on peut compléter en une base de transcendance

$$\widetilde{\mathrm{B}} = \mathrm{B} \sqcup \mathrm{C} = \{b_1, \ldots, b_t\} \sqcup \{c_1, \ldots, c_s\}$$

de K sur k (où $t + s = r = \deg \mathrm{tr}_k \mathrm{K}$). Montrons que L est de degré fini sur $k(\mathrm{B})$. Ceci va résulter du lemme suivant.

Lemme 15.63. — C *est algébriquement indépendante sur* L.

Démonstration. — Sinon, il existe un polynôme $\mathrm{P} \in \mathrm{L}[\mathrm{X}_1, \ldots, \mathrm{X}_s]$ non nul tel que $\mathrm{P}(c_1, \ldots, c_s) = 0$. Sans perte de généralité, on peut supposer que X_s apparaît dans P, et donc que c_s est algébrique sur $\mathrm{L}(\mathrm{C}')$, où $\mathrm{C}' = \{c_1, \ldots, c_{s-1}\}$. Or,

$$\mathrm{L}(c_1, \ldots, c_{s-1}) = k(\mathrm{B} \cup \mathrm{C}')(\mathrm{L})$$

est algébrique sur $k(\mathrm{B} \cup \mathrm{C}')$, puisque L est algébrique sur $k(\mathrm{B})$. Donc, d'après la transitivité des extensions algébriques (15.46), c_s est algébrique sur $k(\mathrm{B} \cup \mathrm{C}')$, une contradiction. Ceci prouve le lemme. □

On peut maintenant achever la preuve du théorème. Soient $\ell_1, \ldots, \ell_n$ des éléments de L linéairement indépendants sur $k(\mathrm{B})$. Montrons qu'ils sont encore linéairement indépendants sur $k(\widetilde{\mathrm{B}})$. Supposons que

$$(*) \qquad 0 = \mathrm{F}_1 \ell_1 + \cdots + \mathrm{F}_n \ell_n,$$

avec $\mathrm{F}_i \in k(\widetilde{\mathrm{B}})$. En chassant les dénominateurs, on se ramène au cas où $\mathrm{F}_i \in k[\widetilde{\mathrm{B}}]$. On peut alors écrire chaque F_i comme une somme finie :

$$\mathrm{F}_i = \sum_{\nu \in \mathbb{N}^s} \mathrm{P}_{i,\nu}(b_1, \ldots, b_t) c_1^{\nu_1} \cdots c_s^{\nu_s}.$$

Alors, $(*)$ entraîne, avec des notations évidentes,

$$0 = \sum_{\nu \in \mathbb{N}^s} \left(\sum_{i=1}^{n} \mathrm{P}_{i,\nu}(b) \ell_i \right) c^\nu.$$

D'après le lemme, on en déduit $\sum_{i=1}^{n} \mathrm{P}_{i,\nu}(b)\ell_i = 0$, pour tout ν, et comme les ℓ_i sont linéairement indépendants sur $k(\mathrm{B})$, il vient $\mathrm{P}_{i,\nu} = 0$ pour tout i, ν, et donc $\mathrm{F}_i = 0$ pour $i = 1, \ldots, n$. Ceci montre que $\ell_1, \ldots, \ell_n$ sont linéairement indépendants sur $k(\widetilde{\mathrm{B}})$. On en déduit que

$$[\mathrm{L} : k(\mathrm{B})] \leqslant [\mathrm{K} : k(\widetilde{\mathrm{B}})].$$

Or, $[\mathrm{K} : k(\widetilde{\mathrm{B}})] < \infty$, d'après le lemme 15.60. Donc L est une extension de degré fini, et a fortiori de type fini, de $k(\mathrm{B})$, et donc L est une extension de type fini de k. Ceci achève la preuve du théorème. □

TABLE DES MATIÈRES

Bibliographie

[Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[Ca] J.-C. Carrega, Théorie des corps – La règle et le compas, Hermann, 1981, 2ème édition 1989.

[ChL] A. Chambert-Loir, Algèbre corporelle, Éditions de l'École Polytechnique, 2005.

[Co] H. S. M. Coxeter, Introduction to Geometry, 2nd edition, Wiley, 1969.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press, 1996.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes, Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Fu] W. Fulton, Algebraic Curves, Benjamin, 1969.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Ne04] J. Nekovář, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~nekovar/co/ln

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Re] M. Reid, Undergraduate commutative algebra, Cambridge Univ. Press, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.

[Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.