III.— Morphismes de corps et extensions finies

Exercice 1 *a) Déterminer les automorphismes du corps* $\mathbb{Q}$.

b) Déterminer les automorphismes du corps $\mathbb{Q}(\sqrt{2})$.

c) Déterminer les automorphismes du corps $\mathbb{R}$. *Indication : Montrer d'abord qu'un tel automorphisme est croissant puis qu'il est continu.*

d) Déterminer les automorphismes continus du corps $\mathbb{C}$.

e) Déterminer les automorphismes de $\mathbb{Q}_p$ *(si on connaît les corps* $p-$*adiques). Indication : vérifier cette caractérisation des unités de l'anneau* $\mathbb{Z}_p$ *: si* $x \in \mathbb{Q}_p$, *alors* $x \in \mathbb{Z}_p^\times \Leftrightarrow x^{p-1}$ *a une racine* $n-$*ième dans* $\mathbb{Q}_p$ *pour une infinités d'entiers* $n > 0$ *; en déduire qu'un automorphisme de* $\mathbb{Q}_p$ *est forcément continu.*

f) Déterminer les morphismes de $\mathbb{Q}(i)$ *dans* $\mathbb{C}$. *Déterminer les morphismes de* $\mathbb{Q}(j)$ *dans* $\mathbb{C}$. *Les corps* $\mathbb{Q}(i)$ *et* $\mathbb{Q}(j)$ *sont-ils isomorphes ?*

g) Déterminer tous les morphismes de corps $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$.

h) Soient p *un nombre premier et* $q := p^n$ *une puissance de* p. *Vérifier que* $F : \mathbb{F}_q \to \mathbb{F}_q$ *est un automorphisme de corps et que* $\mathrm{Aut}(\mathbb{F}_q)$ *est un groupe cyclique d'ordre* n *engendré par* F.

i) Montrer que l'identité est le seul automorphisme du corps $\mathbb{F}_p(t^{\frac{1}{p}})$ *qui laisse fixe les éléments de* $\mathbb{F}_p(t)$.

j) Montrer que $\mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(t)) \simeq \mathrm{PGL}_2(\mathbb{C})$. *Indication : montrer que si* $\frac{p}{q} \in \mathbb{C}(t)$, *alors* $[\mathbb{C}(t) : \mathbb{C}(\frac{p}{q})] = \max\{\deg p, \deg q\}$.

Exercice 2 *a) Déterminer les extensions algébriques de* $\mathbb{R}$.

b) Montrer que l'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ *n'est pas finie.*

c) On pose : $R := \overline{\mathbb{Q}} \cap \mathbb{R}$. *Montrer que* $\overline{\mathbb{Q}} = R(i)$.

Remarque : le théorème d'Artin-Schreier affirme que si K/k *est une extension finie et si* K *est algébriquement clos, alors* k *est de caractéristique* 0, $[K : k] = 2$ *et il existe* $i \in K$ *tel que* $i^2 = -1$ *et* $K = k(i)$.

Théorème de Steinitz

Exercice 3 *Soit* K *un corps.*

a) Si P *est un polynôme de degré* > 0 *sur* K, *montrer qu'il existe une extension algébrique finie de* K *où* P *a une racine.*

b) Soit $\mathscr{P}$ *l'ensemble des polynômes de degré* > 0 *sur* K. *Soit* $A := K[X_f : f \in \mathscr{P}]$. *Montrer que l'idéal de* A *engendré par les* $f(X_f)$, $f \in \mathscr{P}$ *est un idéal propre.*

c) En admettant que tout idéal propre de A *est contenu dans un idéal maximal (cela repose sur le lemme de Zorn), montrer qu'il existe* K_1 *une extension algébrique de* K *où chaque polynôme de* $K[X]$ *de degré* > 0 *a au moins une racine.*

d) En déduire l'existence d'une extension algébrique et algébriquement close de K. Indication : construire une suite croissante par récurrence $K \subseteq K_1 \subseteq K_2 \subseteq ...$ et prendre la réunion des K_i.

Corps finis

Exercice 4 *Soit p un nombre premier.*

a) Montrer que si P est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors P divise $X^{p^n} - X$ sur $\mathbb{F}_p$. Soit $\mathscr{I}_d$ l'ensemble des polynômes unitaires irréductibles de degré d sur $\mathbb{F}_p$. Montrer que :

$$X^{p^n} - X = \prod_{\substack{d|n \\ P \in \mathscr{I}_d}} P \ .$$

b) Soit K un corps fini de carac téristique p. Montrer que K est de cardinal p^n pour un certain n.

c) Montrer qu'il existe un corps de cardinal p^n, unique à isomorphisme près.

Indications : pour l'existence, si Ω est une clôture algébrique de $\mathbb{F}_p$, considérer $\{x \in \Omega : x^{p^n} = x\}$; pour l'unicité, si P est un polynôme irréductible sur $\mathbb{F}_p$ de degré n et si K est un corps de cardinal p^n, montrer que P a au moins une racine x_0 dans K et que le morphisme $\mathbb{F}_p[X]/(P) \to K$, $Q \mapsto Q(x_0)$ est un isomorphisme.

Exercice 5 *Soit P un idéal maximal de $\mathbb{Z}[i]$, l'anneau des entiers de Gauss.*

Montrer que $\mathbb{Z}[i]/P$ est un corps fini de cardinal p où p^2 pour un certain nombre premier p. Déterminer $\mathbb{Z}[i]/(7)$ et $\mathbb{Z}[i]/(2+i)$.