Si $P^\sigma = P$, on a $\left(\frac{P}{Q}\right)^\sigma Q^\sigma = \frac{P}{Q}Q$, donc $P = 0$ ou $Q^\sigma = Q$, puisque $k(X_1, \ldots, X_n)$ est intègre.

Si P et Q ont un facteur commun, quitte à diviser par se facteur, on se ramène au cas où ils n'ont pas de facteur commun non trivial.

Si Q n'est pas symétrique, comme les transpositions engendrent $\mathfrak{S}_n$, il existe une transposition τ telle que $Q^\tau \neq Q$.

Si $\tau = (i, j)$, avec $1 \leqslant i < j \leqslant n$, considérons $P^\tau - P$ (ou $Q^\tau - Q$) comme un polynôme en X_j, à coefficients dans l'anneau $k[X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_n]$. on a $(P^\tau - P)(X_j) \equiv (P^\tau - P)(X_i) \pmod{X_i - X_j}$, or $P^\tau(X_i) = P(X_i)$, donc $X_i - X_j$ divise $P^\tau - P$ (et $Q^\tau - Q$, pour la même raison).

Comme $\left(\frac{P}{Q}\right)^\tau = \frac{P}{Q}$, on a $P^\tau Q = PQ^\tau$, donc $(P^\tau - P)Q = (Q^\tau - Q)P$. En particulier, P divise $(P^\tau - P)Q$ dans l'anneau factoriel $k[X_1, \ldots, X_n]$. Comme P et Q n'ont aucun facteur commun, on trouve que P divise $(P^\tau - P)$.

Le degré en X_m de $\frac{P^\tau - P}{P}$ est inférieur ou égal à 0, pour tout m, donc $\lambda = \frac{P^\tau - P}{P} \in k$.

On a alors $P^\tau - P = \lambda P$ et $Q^\tau - Q = \lambda Q$. Comme $Q \neq Q^\tau$, on a aussi $\lambda \in k^*$.

Comme $X_i - X_j$ divise $(P^\tau - P)$ et $(Q^\tau - Q)$, c'est un facteur commun à P et Q, d'où une contradiction.

Donc Q est symétrique, et donc P l'est aussi d'après la deuxième question.

A.5 Contrôle continu du mardi 14 mars 2006

1. Soient p un nombre premier, et $\mathbb{F}_{p^{10}}$ un corps de p^{10} éléments.

(a) Trouver tous les sous corps $F \subset \mathbb{F}_{p^{10}}$.

(b) Montrer que le groupe $\mathrm{Aut}(\mathbb{F}_{p^{10}})$ de tous les automorphismes de $\mathbb{F}_{p^{10}}$ est cyclique, et trouver tous ses générateurs.

(c) Trouver le nombre de tous les polynômes unitaires irréductibles de degré 10 sur $\mathbb{F}_{p^{10}}$.

2. a) Trouver le terme constant du polynôme minimal P sur $\mathbb{Q}$ du nombre algébrique $\alpha = \sqrt{2} + \sqrt[3]{3}$.

b) Trouver toutes les racines complexes de P.

c) Déterminer le groupe de Galois du corps engendré par toutes les racines complexes de P.

3.* On considère une extension galoisienne L/K de groupe de Galois $\mathrm{Gal}(L/K)$, isomorphe au groupe symétrique S_5.

a) Déterminer toutes les sous-extensions galoisiennes E/K, où $K \subset E \subset L$.

b) Donner un exemple de deux sous-extensions E_1/K et E_2/K, ($E_1 \subset L$, $E_2 \subset L$) telles que E_1 et E_2 ne sont pas incluses l'une dans l'autre, le composé $E_1 \cdot E_2$ n'est pas égal à L, et l'intersection $E_1 \cap E_2$ n'est pas égale à K.

2006

4.* On considère le polynôme à coefficients rationnels

$$P(T) = T^3 - 3T - 1.$$

(a) Trouver le discriminant de P.

(b) Montrer que P est irréductible sur $\mathbb{Q}$ et qu'il possède trois racines réelles α_1, α_2, α_3, telles que $\alpha_3 < \alpha_2 < 0 < \alpha_1$.

(c) Montrer que si α est racine P, il en est de même de $2 - \alpha^2$. On pose $K = \mathbb{Q}(\alpha_1)$.

(d) Montrer que l'extension $K/\mathbb{Q}$ est galoisienne, et que tout élément de son groupe de Galois induit une permutation paire sur l'ensemble $\{\alpha_1, \alpha_2, \alpha_3\}$.

Références

Ouvrages de base :

[Bosch] Siegfried Bosch, *Algebra*, 3rd Ed., 1999

[Bourbaki] Bourbaki N. *Algèbre, Chap.8 . "Modules et anneaux semi-simples"*, Masson, Paris 1981.

[Dieudonné] Jean Alexandre Dieudonné, *La géométrie des groupes classiques*, Springer, 1963.

[Godement] Roger Godement, *Cours d'algèbre.*, Hermann, Paris, 1969

[Lang] Serge Lang , *Algebra.* Reading, Mass. : Addison–Wesley, 3rd Ed., 1993.

[Se70] Jean– Pierre Serre, *Cours d'arithmétique.* Paris, Press Univ. France, 1970.

[VdW71] B.L. van der Waerden, *Algebra I,II*, New York : Springer Verlag, 1971, 1967.

Lectures complémentaires :

[AMcD] I. G. MacDonald et M. F.Atiyah, *Introduction to Commutative Algebra.* Reading, MA : Addison-Wesley, 1969.

[Bigard] Alain Bigard, Géométrie, Cours et exercices corrigés pour le Capes et l'agrégation, Masson, 1998

[BS85] Z.I. Borevich, I.R.Shafarevich, *Number Theory.* Traduction anglaise. : New York/London : Academic Press, 1966.

[ChL] Antoine Chambert-Loir *Algèbre commutative*, `http ://www.polytechnique.fr/ chambert/ teach/algcom.pdf`

[Coq02] Robert Coquereaux, *Espaces fibrés et connexions. Une introduction aux géométries classiques et quantiques de la physique théorique.* Centre de Physique Théorique, Luminy - Marseille, `http ://www.cpt.univ-mrs.fr/~coque/book/sourceforhtml.html`

[Garrett] Paul Garrett's Page `http ://www.math.umn.edu/~garrett/m/buildings/`

2006

[Jac] N. Jacobson, *Basic Algebra I and II*, New York, NY : W.H. Freeman, 1974, 1989. Second Edition.

[Kob87] Neal Koblitz, *A course of number theory and cryptography*, Graduate texts in mathematics 114, New York : Springer Verlag, 1987.

[Kos82] A.I. Kostrikin, *Introduction to Algebra New York*, NY : Springer-Verlag, 1982

[KosMan] A.I. Kostrikin, Yu. I. Manin, *Linear algebra and geometry*, Nauka, Moscow 1986 ; English translation, Gordon and Breach, New York-London 1989

[Li-Ni] Rudolf Lidl et Harald Niederreiter, *Introduction to finite fields and their applications.* Addison–Wesley : Reading, 1983

[Ma-Pa] Yu.I. Manin et A.A.Panchishkin, *Introduction to Modern Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49 (2nd ed.), Springer-Verlag, 2005, 514 p.

[Mi-Hu] J. Milnor et D.Hüsemoller, *Symmetric bilinear forms*, Springer-Verlag, 1973

[Sha87] I.R. Shafarevich, (1987) : Fundamental notions of algebra. Itogi Nauki, 11, 1987. English transl. : Encycl. Math. Sci 11. Berlin–Heidelberg–New York : Springer–Verlag, 1990.

[Weyl] Hermann Weyl, The Classical Groups : Their Invariants and Representations

[Tits] Jacques Tits, *Le Monstre (d'après R. Griess, B. Fischer et al.)* dans Séminaire Bourbaki, Vol. 1983/84. Astérisque no 121-122, (1985), 105–122.

[Wei74] A.Weil (1974) : Basic Number Theory. 3rd ed. Berlin–Heidelberg–New York : Springer–Verlag, 1974.

[W] Wikipédia, *Wikipédia, l'encyclopédie libre*
`http ://fr.wikipedia.org/wiki)`

[Stein] William Stein, *An Explicit Approach to Number Theory* (à paraître, voir page internet : `http ://modular.fas.harvard.edu/edu/Fall2001/124/lectures`).