École Polytechnique 2009-2010
Théorie de Galois

Feuille d'exercices 2

Exercice 1. (Rappels de cours). Soit A un anneau et I un idéal de A. On dit que I est premier si $xy \in I$ implique $x \in I$ ou $y \in I$. On dit que I est maximal si $I \neq A$ et si pour J idéal tel que $I \subsetneq J \subseteq A$, on a $J = A$.

(i) Montrer que I est premier si et seulement si A/I est intègre.

(ii) Montrer que I est maximal si et seulement si A/I est un corps.

(iii) Montrer qu'un idéal maximal est premier.

On pose $A = \mathbf{Z}$. On rappelle que les idéaux de $\mathbf{Z}$ sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$.

(iv) Soit $n > 0$. Montrer que $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si c'est un corps. A quelle condition sur n est-ce réalisé ?

Exercice 2. Soit A un anneau et $A[T]$ l'anneau des polynômes à coefficients dans A.

(i) Quels sont les éléments inversibles de $A[T]$?

(ii) Montrer que $A[T]$ est intègre si et seulement si A est intègre.

On pose à présent $A = \mathbf{Z}$. On dit qu'un polynôme $P(T) \in \mathbf{Z}[T]$ non nul est primitif si tous ses coefficients sont premiers entre eux dans leur ensemble.

(iii) Montrer que le produit de deux polynômes primitifs est primitif.

(iv) Montrer que tout polynôme non nul P de $\mathbf{Q}[T]$ s'écrit de maniere unique sous la forme $P = c(P)Q$ avec Q dans $\mathbf{Z}[T]$ primitif et $c(P) \in \mathbf{Q}_{>0}$. Vérifier que $c(P) \in \mathbf{Z}$ si $P \in \mathbf{Z}[T]$.

Le rationel $c(P)$ s'appelle le contenu de P.

(v) Montrer que pour $P, Q \in \mathbf{Q}[T]$, $c(PQ) = c(P)c(Q)$.

Exercice 3. Un polynôme $P \in \mathbf{Z}[T]$ est dit irréductible dans $\mathbf{Z}[T]$ si il ne se factorise pas sous la forme $P = QR$ avec $Q, R \in \mathbf{Z}[T]$ non inversibles dans $\mathbf{Z}[T]$.

(i) (Lemme de Gauss) Montrer qu'un polynôme $P \in \mathbf{Z}[T]$ non constant est irréductible si et seulement si il est primitif et irréductible en tant que polynôme de $\mathbf{Q}[T]$. On pourra utiliser l'exercice précédent.

(ii) Soit $P = a_0 + a_1T + \cdots + a_nT^n \in \mathbf{Z}[T]$ un polynôme primitif non constant. Supposons qu'il existe un nombre premier p tel que p divise $a_0, a_1, \cdots, a_{n-1}$, p ne divise pas a_n, et p^2 ne divise pas a_0. Montrer que P est irréductible dans $\mathbf{Z}[T]$.

(iii) (Critère d'Eisenstein) On enlève l'hypothèse que P est primitif. Montrer que P est irréductible dans $\mathbf{Q}[T]$.

Exercice 4. Montrer que le polynôme $T^4 + T + 1$ est irréductible dans $\mathbf{Q}[T]$.

Exercice 5. (i) Lister les polynômes irréductibles de degré ≤ 3 dans $(\mathbf{Z}/2\mathbf{Z})[T]$.

(ii) Montrer que le polynôme $T^5+3T^4-2T^3+4T^2-2T+3$ est irréductible dans $\mathbf{Q}[T]$. On pourra d'abord étudier ses réductions modulo 2 et 3 (on admettra éventuellement que T^4+T^2+T+1 est irréductible dans $(\mathbf{Z}/3\mathbf{Z})[T]$).

Exercice 6. (i) Montrer que les $\mathbf{R}$-algèbres $\mathbf{R} \times \mathbf{R}$, $\mathbf{C}$ et $\mathbf{R}[X]/(X^2)$ ne sont pas isomorphes (on pourra considérer leurs diviseurs de 0 et leurs éléments nilpotents).

(ii) Soient $a, b \in \mathbf{R}$. Montrer que $\mathbf{R}[X]/(X^2 + aX + b)$ est isomorphe à l'une de ces trois $\mathbf{R}$-algèbres.

(iii) En déduire qu'à isomorphisme près, toute $\mathbf{R}$-algèbre de dimension 2 est isomorphe à une, et une seule, des algèbres du (i).

(iv) (plus difficile) Montrer qu'à isomorphisme près il y a cinq $\mathbf{R}$-algèbres commutatives de dimension 3.

Exercice 7. Soit A la $\mathbf{R}$-algèbre des fonctions $\mathbf{R} \to \mathbf{R}$ qui sont 2π-périodiques et $B \subset A$ sa sous-algèbre des polynômes trigonométriques.

(i) Montrer que

$$B \simeq \mathbf{R}[X, Y]/(X^2 + Y^2 - 1).$$

(On pourra remarquer que tout $P \in \mathbf{R}[X, Y]$ s'écrit sous la forme $(X^2+Y^2-1)A + XP + Q$ où $A \in \mathbf{R}[X, Y]$ et $P, Q \in \mathbf{R}[Y]$).

(ii) En déduire que $(X^2 + Y^2 - 1)$ est un idéal premier de $\mathbf{R}[X, Y]$, et qu'il est non maximal.

Exercice 8. (i) Montrer qu'il existe des polynômes irréductibles dans $\mathbf{Q}[T]$ de tout degré.

(ii) (plus difficile) Mieux, montrer que si l'on identifie les polynômes unitaires de degré n à coefficients dans $\mathbf{Q}$ à $\mathbf{Q}^n$ au moyen de la suite de leurs coefficients, alors les polynômes irréductibles sont denses dans $\mathbf{Q}^n$. (Si $P \in \mathbf{Q}[T]$ est fixé, on pourra appliquer le critère d'Eisenstein au polynôme $X^nQ(1/X)$ où $Q = P + 1/p$ pour p premier assez grand).