École polytechnique 2012-2013
Théorie de Galois

Feuille d'exercices 2

Les anneaux sont supposés commutatifs et unitaires.

Exercice 1. (Lemme de Cauchy) Soient G un groupe fini et p un nombre premier divisant $|G|$. On se propose de montrer que G contient un élément d'ordre p.

i. On considère $X = \{(x_1, \ldots, x_p) \in G^p, x_1 \cdots x_p = 1\}$. Calculer $|X|$.

ii. Montrer que $(i, (x_j)) \mapsto (x_{j+i})$ (les indices étant pris modulo p) définit une action du groupe $\mathbf{Z}/p$ sur l'ensemble X.

iii. Conclure en utilisant la congruence $|X| = |X^{\mathbf{Z}/p}| \mod p$.

Exercice 2. Soit p un nombre premier. Montrer que tout p-groupe fini est résoluble.

Exercice 3. (Contenu de Gauß d'un polynôme)
On dit qu'un polynôme $P(T) \in \mathbf{Z}[T]$ non nul est *primitif* si ses coefficients sont premiers entre eux dans leur ensemble.

i. Montrer que le produit de deux polynômes primitifs est primitif. (On pourra réduire modulo des nombres premiers ou utiliser le résultat de l'exercice 5.)

ii. Montrer que tout polynôme non nul P de $\mathbf{Q}[T]$ s'écrit de manière 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 rationnel $c(P)$ s'appelle le *contenu* de P.

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

iv. (Lemme de Gauß, forme usuelle) 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 et R différents de ± 1. Montrer que si P est irréductible dans $\mathbf{Z}[T]$, alors il est irréductible dans $\mathbf{Q}[T]$.

Exercice 4. (Lemme de McCoy-永田)
Soit A un anneau commutatif. On veut montrer qu'un polynôme $P \in A[X]$ non nul est diviseur de zéro si et seulement si il existe $a \neq 0$ dans A tel que $aP = 0$.

i. Écrivons $P = a_0 + a_1 X + \cdots + a_n X^n$ et considérons $Q = b_0 + b_1 X + \cdots + b_m X^m \neq 0$ tel que $PQ = 0$. Montrer que si $Pb_m \neq 0$, il existe un plus grand indice $d \leq n$ tel que $a_d Q \neq 0$.

ii. Montrer que le degré de $a_d Q$ est strictement inférieur à m.

iii. Conclure par récurrence sur le degré de Q.

Exercice 5. (Anneaux quotients et lemme de Gauß universel)
Soient n et m des entiers et R l'anneau quotient de $\mathbf{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m, A_0, \ldots, A_n, B_0, \ldots, B_m]$ par l'idéal engendré par les éléments $1 - \sum_0^n a_i A_i$, $1 - \sum_0^m b_m B_m$ et les $C_k = \sum_{i+j=k} A_i B_j$ pour $0 \leq k \leq n + m$. Enfin, soient $A = \sum_0^n \overline{A_i} X^i$ et $B = \sum_0^m \overline{B_j} X^j$ les polynômes dans $R[X]$.

i. Montrer que $AB = 0$.

ii. Montrer que les coefficients de A (resp. B) engendrent l'idéal unité de R.

iii. En déduire, en utilisant le lemme de McCoy-永田, que l'anneau R est nul.

iv. On dit un polynôme à coefficients dans un anneau (quelconque) est *primitif* si l'idéal engendré par ses coefficients est l'anneau tout entier. Déduire de ce qui précède que le produit de deux polynômes *primitifs* est primitif.

Exercice 6. (Critère de [Schönemann-]Eisenstein)

i. Soit $P = a_0 + a_1 T + \cdots + a_n T^n \in \mathbf{Z}[T]$ un polynôme 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 $\mathbf{Q}[T]$. (On pourra utiliser le lemme de Gauß.)

ii. Montrer que pour tout entier n, il existe un polynôme irréductible de degré n dans $\mathbf{Q}[T]$.

Exercice 7. (Comptage et réduction modulo p)

i. Lister les polynômes irréductibles unitaires de degré ≤ 3 dans $\mathbf{F}_2[T]$ et ceux de degré ≤ 2 dans $\mathbf{F}_3[T]$.

ii. Montrer que $T^4 + T^2 + T + 1$ est irréductible dans $\mathbf{F}_3[T]$.

iii. Montrer que le polynôme $T^5 + 3T^4 - 2T^3 + 4T^2 - 2T + 3$ est irréductible dans $\mathbf{Q}[T]$.

iv. Soit p un nombre premier. Montrer que le nombre de polynômes irréductibles unitaires de degré ≤ 3 dans $\mathbf{F}_p[T]$ est $\frac{1}{3}p^3 + \frac{1}{2}p^2 + \frac{1}{6}p$.

v. Est-il vrai que le nombre de polynômes irréductibles unitaires de degré d dans $\mathbf{F}_p[T]$ est un polynôme en p ?

Exercice 8.

i. Montrer que $K = \mathbf{Q}(\sqrt{5}, \sqrt[5]{2})$ est de degré 10 sur $\mathbf{Q}$.

ii. En déduire que K est isomorphe à la $\mathbf{Q}$-algèbre $\mathbf{Q}[X, Y]/(X^2 - 5, Y^2 - 5)$.

iii. En déduire un procédé permettant de trouver un polynôme annulateur de $\alpha = \sqrt{5} + \sqrt[5]{2}$.

iv. Comment pourrait-on vérifier que le polynôme

$$P = X^{10} - 25\,X^8 + 250\,X^6 - 4\,X^5 - 1250\,X^4 - 200\,X^3 + 3125\,X^2 - 500\,X - 3121$$

convient ?

Exercice 9.

i. Soient k un corps et A une k-algèbre de dimension finie. Montrer que l'ensemble $\mathrm{Specmax}(A)$ des idéaux maximaux de A est fini, de cardinal au plus $[A : k] = \dim_k(A)$. (Indication : on pourra utiliser le théorème chinois.)

ii. À quelle condition a-t-on égalité ?

Exercice 10. Soit A un anneau commutatif. On rappelle qu'un *idempotent* de A est un élément e tel que $e^2 = e$.

i. Montrer que l'ensemble $B = \mathrm{Idem}(A)$ muni de l'addition $e \boxplus e' := (e - e')^2$ et de la multiplication $e \boxtimes e' := ee'$ est un anneau.

ii. Montrer que tout idéal premier $\mathfrak{p}$ de B est maximal, et que $B/\mathfrak{p}$ est isomorphe à $\mathbf{F}_2$.

iii. Montrer que l'ensemble $\pi_0(A) = \mathrm{Spec}(\mathrm{Idem}(A))$ des idéaux premiers de $\mathrm{Idem}(A)$ est un singleton si et seulement si A a exactement deux idempotents.