Université Bordeaux 1 — **Master CSI**
Mathématiques — M1MA7W01
Année 2011-2012 — **Arithmétique**

Devoir Surveillé du 9 novembre 2011

Corrigé

Exercice 1 – *On considère dans* $\mathbb{F}_5[X]$ *le polynôme* $P(X) = X^3 - X + 1$ *et on note* A *l'anneau* $\mathbb{F}_5[X]/(P(X))$.

1) *Quelle est la caractéristique de* A *? Quel est son cardinal ? Montrer que* A *n'est pas un corps.*

On a trivialement $\mathrm{car}(A) = 5$ et $\mathrm{card}(A) = 5^3 = 125$. Comme $X^3 - X + 1 = (X + 2)(X^2 + 3X + 3)$ dans $\mathbb{F}_5[X]$, $P(X)$ n'est pas irréductible et A n'est pas un corps.

2) *Déterminer dans* $\mathbb{F}_5[X]$ *les polynômes unitaires de degré* $\leqslant 2$ *non premiers avec* $P(X)$.

On vérifie que X^2+3X+3 n'a pas de racine dans $\mathbb{F}_5$, et est donc irréductible dans $\mathbb{F}_5[X]$ car de degré 2. Les polynômes recherchés sont les multiples unitaires de $X+2$ et X^2+3X+3 de degré $\leqslant 2$. Ce sont $X+2$, $X(X+2) = X^2+2X$, $(X+1)(X+2) = X^2+3X+2$, $(X+2)(X+2) = X^2+4X+4$, $(X+3)(X+2) = X^2+1$, $(X+4)(X+2) = X^2+X+3$ (les multiples de $X+2$) et X^2+3X+3 (le seul multiple unitaire de degré $\leqslant 2$ de X^2+3X+3).

3) *En déduire le cardinal de* $A^\times$.

Les éléments de $A^\times$ correspondent aux polynômes de degré $\leqslant 2$ premiers avec $P(X)$. Il faut donc exclure les polynômes non premiers avec $P(X)$. Il y a 0 et les polynômes précédents multipliés par une constante non nulle (4 possibilités). On en a donc $1+4\times 7 = 29$. Par suite $\mathrm{car}(A^\times) = 125 - 29 = 96$.

4) *Calculer* X^5, X^{10} *et* X^{25} *modulo* $P(X)$ *et montrer que pour tout* $\xi \in A$ *on a* $\xi^{25} = \xi$.

Soit α la classe de X dans A. On a $\alpha^3 = \alpha - 1$ d'où $\alpha^4 = \alpha^2 - \alpha$. Le calcul donne

$$\alpha^5 = \alpha^3 - \alpha^2 = -\alpha^2 + \alpha - 1,$$

puis

$$\alpha^{10} = \alpha^4 + \alpha^2 + 1 - 2\alpha^3 + 2\alpha^2 - 2\alpha = 4\alpha^2 - 5\alpha + 3 = 4\alpha^2 + 3.$$

Enfin, $\alpha^{25} = -\alpha^{10} + \alpha^5 - 1$ car A est de caractéristique 5 et cela conduit à

$$\alpha^{25} = -4\alpha^2 - 3 - \alpha^2 + \alpha - 1 - 1 = \alpha.$$

Tout $\xi \in A$ s'écrit $a\alpha^2 + b\alpha + c$ où $(a, b, c) \in \mathbb{F}_5^3$. Comme A est de caractéristique 5, on a

$$\xi^{25} = a^{25}\alpha^{50} + b^{25}\alpha^{25} + c^{25},$$

ce qui donne par ce qui précède et par $x^5 = x$ pour tout $x \in \mathbb{F}_5$,

$$\xi^{25} = a\alpha^2 + b\alpha + c = \xi.$$

5) *Le groupe $A^\times$ est-il cyclique ?*

Non, sinon il contiendrait un élément d'ordre multiplicatif son cardinal i.e. 96. Or par la question précédente, si $\xi \in A^\times$ on a $\xi^{24} = 1$ et l'ordre de ξ divise 24.

6) *Quels sont a priori les ordres possibles des éléments de $A^\times$? Montrer que la classe de X dans A est un élément de $A^\times$ d'ordre maximal, et que pour chaque ordre possible d précédemment recensé, il existe dans $A^\times$ un élément d'ordre d.*

On vient de voir que ce sont les diviseurs de 24, à savoir 1, 2, 3, 4, 6, 8, 12, 24. Pour montrer que α est d'ordre maximal i.e. 24, il suffit de vérifier que $\alpha^8 \neq 1$ et $\alpha^{12} \neq 1$. Or le calcul donne par exemple

$$\alpha^8 = \alpha^3\alpha^5 = (\alpha - 1)(-\alpha^2 + \alpha - 1) = -\alpha^3 + 2\alpha^2 - 2\alpha + 1 = 2\alpha^2 - 3\alpha + 2 \neq 1,$$

et

$$\alpha^{12} = \alpha^2\alpha^{10} = \alpha^2(4\alpha^2 + 3) = 4\alpha^4 + 3\alpha^2 = 4\alpha^2 - 4\alpha + 3\alpha^2 = 2\alpha^2 + \alpha \neq 1.$$

Soit d un des ordres possibles. Alors $\alpha^{24/d}$ est d'ordre d car α est d'ordre 24.

Exercice 2 – *On considère dans $\mathbb{F}_2[X]$ le polynôme $P(X) = X^6 + X^5 + 1$ et on note A l'anneau $\mathbb{F}_2[X]/(P(X))$.*

1) *Soit α la classe de X dans A. Montrer que $\alpha \in A^\times$ et calculer l'ordre de α dans $A^\times$ (on pourra calculer successivement α^7, α^8, α^9, α^{10}, α^{11}, α^{21} et α^{63}).*

Comme $\mathrm{pgcd}(X, X^6 + X^5 + 1) = 1$, $\alpha \in A^\times$. On a $\alpha^6 = \alpha^5 + 1$ donc

$$\alpha^7 = \alpha^6 + \alpha = \alpha^5 + \alpha + 1,$$
$$\alpha^8 = \alpha^6 + \alpha^2 + \alpha = \alpha^5 + \alpha^2 + \alpha + 1,$$
$$\alpha^9 = \alpha^6 + \alpha^3 + \alpha^2 + \alpha = \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\alpha^{10} = \alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\alpha^{11} = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1.$$

On en tire

$$\alpha^{21} = \alpha^{10}\alpha^{11} = \alpha^9 + \alpha^8 + \alpha^7 + \alpha^6 + \alpha^5 + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)^2.$$

Comme on est en caractéristique 2, ce carré vaut $\alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 + 1$, et finalement

$$\alpha^{21} = \alpha^9 + \alpha^7 + \alpha^5 + \alpha^4 + \alpha^2 + 1 = \alpha^5 + \alpha^4 + \alpha^3 + 1.$$

On en tire

$$\alpha^{42} = \alpha^{10} + \alpha^8 + \alpha^6 + 1 = \alpha^5 + \alpha^4 + \alpha^3,$$

et

$$\alpha^{63} = (\alpha^5 + \alpha^4 + \alpha^3)^2 + \alpha^5 + \alpha^4 + \alpha^3 = \alpha^{10} + \alpha^8 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 = 1.$$

Lordre de α divise $63 = 3^2 \cdot 7$. Comme $\alpha^9 \neq 1$ et $\alpha^7 \neq 1$, l'ordre de α vaut 63.

2) *En déduire que A est un corps. On identifiera A à $\mathbb{F}_{64}$.*

Comme $\alpha \in A^\times$ et est d'ordre 63, le sous-groupe multiplicatif de $A^\times$ qu'il engendre a pour cardinal 63. Or le cardinal de $A\backslash\{0\}$ est $2^6 - 1 = 63$. On a donc $A^\times = A\backslash\{0\}$ et A est un corps.

3) *Montrer que $P(X)$ est irréductible et primitif.*

Comme $A = \mathbb{F}_2[X]/(P(X))$ est un corps $P(X)$ est irréductible. En outre, on vient de voir que la classe de X est d'ordre 63, donc est un élément primitif de $\mathbb{F}_{64}$. Ainsi $P(X)$ est irréductible et primitif.

4) *Combien y a-t-il de polynômes irréductibles de degré 6 dans $\mathbb{F}_2[X]$?*

On sait que $X^{64} - X$ est le produit des polynômes irréductibles (unitaires) de $\mathbb{F}_2[X]$ de degrés 1, 2, 3 et 6. Il y a 2 polynômes de degré 1 irréductibles à savoir X et $X + 1$. Il y a un seul polynôme irréductible de degré 2 à savoir $X^2 + X + 1$ et deux polynômes irréductibles de degré 3, à savoir $X^3 + X^2 + 1$ et $X^3 + X + 1$. On en déduit qu'il y a $(64 - 2 \times 1 - 1 \times 2 - 2 \times 3)/6 = 9$ polynômes irréductibles de degré 6 dans $\mathbb{F}_2[X]$.

5) *Combien y a-t-il de polynômes irréductibles primitifs de degré 6 dans $\mathbb{F}_2[X]$?*

On sait qu'il y a $\varphi(p^n - 1)/n$ polynômes unitaires irréductibles primitifs de degré n dans $\mathbb{F}_p[X]$. Ici avec $p = 2$ et $n = 6$, on a $\varphi(63)/6 = \varphi(3^2 \cdot 7)/6 = (2 \cdot 3 \cdot 6)/6 = 6$ polynômes irréductibles primitifs (unitaires) de degré 6 dans $\mathbb{F}_2[X]$.

6) *Quels sont les sous-corps de A ?*

Les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ où d divise n. Ici, avec $p = 2$ et $n = 6$, on obtient $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_{64}$ lui-même.

7) *On pose $\beta = \alpha^5 + \alpha^4 + \alpha^3$. Montrer que β appartient à un sous-corps strict de A à préciser.*

Soit, on reconnaît α^{42} et alors on voit que $\beta^2 = \alpha^{84} = \alpha^{21}$ puis que $\beta^4 = \alpha^{42} = \beta$. Soit on calcule β^2 puis β^4 à partir des relations obtenues en Question 1. Comme $\beta^4 = \beta$, on a $\beta \in \mathbb{F}_4$.

8) *Quel est le polynôme minimal de β sur $\mathbb{F}_2$?*

On a $P_\beta(X) = (X - \beta)(X - \beta^2) = X^2 - (\beta + \beta^2) + \beta^3$. Mais $\beta^4 = \beta$ et $\beta \neq 0$ implique $\beta^3 = 1$. De plus $\beta + \beta^2 = \alpha^{42} + \alpha^{21} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^5 + \alpha^4 + \alpha^3 + 1 = 1$. Finalement $P_\beta(X) = X^2 + X + 1$.

9) *On pose $\gamma = \alpha^5 + \alpha^2 + 1$. Combien le corps $\mathbb{F}_2(\gamma)$ compte-t-il d'éléments ?*

Par un calcul faisant appel aux résultats de la Question 1, on obtient : $\gamma^2 = \alpha^5 + \alpha^3 + \alpha^2 + \alpha$ puis $\gamma^4 = \alpha^3 + \alpha$ et $\gamma^8 = \alpha^5 + \alpha^2 + 1 = \gamma$. Ceci montre que $\gamma \in \mathbb{F}_8$ et $\gamma \notin \mathbb{F}_4$. L'extension $\mathbb{F}_2(\gamma)$ est un sous-corps de $\mathbb{F}_{64}$ qui est inclus dans $\mathbb{F}_8$ mais pas dans $\mathbb{F}_4$. On a donc $\mathbb{F}_2(\gamma) = \mathbb{F}_8$ qui compte 8 éléments.

10) *Déterminer* $\mathbb{F}_2(\beta) \cap \mathbb{F}_2(\gamma)$.

Comme $\mathbb{F}_2(\beta) = \mathbb{F}_4$ l'intersection cherchée est un sous-corps de $\mathbb{F}_{64}$ inclus à la fois dans $\mathbb{F}_8$ et dans $\mathbb{F}_4$. Comme sous-corps de $\mathbb{F}_8$ et de $\mathbb{F}_4$, il est de la forme $\mathbb{F}_{2^d}$ où d divise 3 et 2. Seule posssibilité : $d = 1$. On a $\mathbb{F}_2(\beta) \cap \mathbb{F}_2(\gamma) = \mathbb{F}_2$

Exercice 3 –

1) *Montrer que dans* $\mathbb{F}_2[X]$ *le polynôme* $X^4 + X^3 + X^2 + X + 1$ *est irréductible.*

Il suffit de vérifier qu'il n'est divisible par aucun polynôme irréductible de degré $\leqslant 2$ à savoir X, $X + 1$ et $X^2 + X + 1$, ce qui se fait sans peine.

2) *À l'aide des classes cyclotomiques binaires modulo 7 (respectivement modulo 11), étudier la décomposition en produit d'irréductibles de* $X^6 + X^5 + \cdots + X + 1$ *(respectivement* $X^{10} + X^9 + \cdots + X + 1$*) dans* $\mathbb{F}_2[X]$*. On ne demande pas ici d'expliciter la décomposition mais juste de donner le nombre de facteurs irréductibles et leurs degrés.*

Notons que si n est impair, les classes cyclotomiques binaires modulo n donnent le profil de la décomposition de $X^n - 1$ dans $\mathbb{F}_2[X]$ car $\text{pgcd}(n, 2) = 1$. Ce sera le cas dans toutes les questions qui suivent. Les classes cyclotomiques binaires modulo 7 sont $\{0\}$, $\{1, 2, 4\}$, $\{3, 6, 5\}$. Pa suite, le polynôme $X^7 - 1$ se décompose en produit de 3 polynômes irréductibles (unitaires), l'un de degré 1 (nécessairement $X + 1 = X - 1$), les deux autres de degré 3. Comme $X^6 + X^5 + \cdots + X + 1 = (X^7 - 1)/(X - 1)$, le polynôme $X^6 + X^5 + \cdots + X + 1$ de décompose en produit de deux irréductibles de degré 3.

3) *Montrer que si* p *est premier impair on a l'équivalence :*
$X^{p-1} + X^{p-2} + \cdots + X + 1$ *est irréductible dans* $\mathbb{F}_2[X]$ *si et seulement si 2 est racine primitive modulo* p*.*

Supposons que 2 soit racine primitive modulo p. Alors 2 engendre $\mathbb{F}_p^\times$ et la classe binaire cyclotomique modulo p de 1, i.e. $\{2^i \bmod p;\ i \neq 0\}$ est $\mathbb{F}_p^\times$ entier. Les classes binaires cyclotomiques modulo p sont $\{0\}$ et $\mathbb{F}_p^\times$. Par conséquent, $X^p - 1$ est produit d'un polynôme irréductible (unitaire) de degré 1, nécessairement $X + 1 = X - 1$ et d'un polynôme irréductible (unitaire) de degré $p - 1$ qui vaut donc $(X^p - 1)/(X - 1)$. Or ce dernier quotient est $X^{p-1} + X^{p-2} + \cdots + X + 1$ qui est donc irréductible. Réciproquement si ce polynôme noté $P(X)$ est irréductible, $X^p - 1$ est produit de $X - 1$ qui est irréducible (unitaire) et du polynôme irréductible (unitaire) $P(X)$. Il y a donc deux classes binaires cyclotomiques modulo p, $\{0\}$ et nécessairement $\mathbb{F}_p^\times$. Mais cette dernière classe, qui peut être vue comme celle de 1 est formée des $2^i \bmod p$ ($i \geqslant 0$). Ainsi tout élément de $\mathbb{F}_p^\times$ est une puissance de 2 qui est donc une racine primitive modulo p.

4) *Étudier les cas* $p = 13, 17$.

Modulo 13 les puissances de 2 sont 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7. Ainsi 2 engendre $\mathbb{F}_{13}^\times$ et 2 est racine primitive modulo 13. Par suite $X^{12} + X^{11} + \cdots + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.
Modulo 17 les puissances de 2 sont 1, 2, 4, 8, 16, 15, 13, 9 : le sous-groupe de $\mathbb{F}_{17}^\times$ engendré par 2 n'est pas $\mathbb{F}_{17}^\times$ entier. Ainsi 2 n'est pas racine primitive modulo 17 et

$X^{16} + X^{15} + \cdots + X + 1$ n'est pas irréductible dans $\mathbb{F}_2[X]$. On peut être plus précis. En s'inspirant de ce qui a été fait plus haut, les classes cyclotomiques binaires modulo 17 sont $\{0\}$, $\{1, 2, 4, 8, 16, 15, 13, 9\}$, $\{3, 6, 12, 7, 14, 11, 5, 10\}$ et en fait $X^{16} + X^{15} + \cdots + X + 1$ est produit de deux irréductibles de degré 8.

5) *Montrer que si n est un entier impair $\geqslant 3$, on a plus généralement :*
$X^{n-1} + X^{n-2} + \cdots + X + 1$ *est irréductible dans* $\mathbb{F}_2[X]$ *si et seulement si n est premier et 2 est racine primitive modulo n.*

L'implication $\Leftarrow$ a été établie dans la Question 3. Supposons maintenant que $X^{n-1} + X^{n-2} + \cdots + X + 1$ soit irréductible dans $\mathbb{F}_2[X]$. La décomposition de $X^n - 1$ en produit d'irréductibles est $(X-1)(X^{n-1} + X^{n-2} + \cdots + X + 1)$. Il y a donc deux classes cyclotomiques binaires modulo n, la classe triviale $\{0\}$ et nécessairement $\mathbb{Z}/n\mathbb{Z}\backslash\{0\}$. Et cette dernière qui est la classe de 1 est constituée des puissances de 2 modulo n. Comme 2 est inversible modulo n impair, toutes ses puissances le sont et tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible. Par suite n est premier. Le fait que 2 soit racine primitive modulo n a été vu en Question 3.