Université de Bretagne Occidentale
UFR Sciences et Techniques
L3 DE MATHEMATIQUES

ARITHMÉTIQUE ET APPLICATIONS

Contrôle continu, le 16 février 2023, 8h00-8h30

CORRIGE

Documents de CM et de TD autorisés. Calculatrices interdites.

Exercice 1. a. D'après le cours, on sait que le groupe $\mathbb{F}_{49}^\times$ est cyclique d'ordre $49-1=48=2^4\times 3$. Le nombre de générateurs de $\mathbb{F}_{49}^\times$ est donc $\varphi(48)=\varphi(2^4)\times\varphi(3)=2^3\times(3-1)=16$.

b. Le polynôme $X^2+1\in\mathbb{F}_7[X]$ n'a pas de racine dans $\mathbb{F}_7$ car

$$0^2+1=1\neq 0,\ (\pm 1)^2+1=2\neq 0,\ (\pm 2)^2+1=5\neq 0\quad\text{et}\quad(\pm 3)^2+1=3\neq 0$$

dans $\mathbb{F}_7$. Comme il est de degré 2, cela suffit pour conclure qu'il est irréductible [1]. On pose donc $\mathbb{F}_{49}=\mathbb{F}_7[X]/(X^2+1)$.

c. Comme $|\mathbb{F}_{49}^\times|=48=2^4\times 3$. Les diviseurs maximaux [2] non triviaux de 48 sont $\frac{48}{2}=24$ et $\frac{48}{3}=16$. D'après le cours un élément x de $\mathbb{F}_{49}^\times$ est donc un générateur de $\mathbb{F}_{49}^\times$ si et seulement si $x^{24}\neq 1$ et $x^{16}\neq 1$.

d. On a $\bar{X}^2=-1$ dans $\mathbb{F}_{49}$. Du coup $\bar{X}^4=1$, et $\bar{X}$ n'est donc certainement pas un générateur de $\mathbb{F}_{49}^\times$.

Regardons si $\bar{X}+1$ en est un. Lorsqu'on commence à calculer $(\bar{X}+1)^{16}$ par carrés répétés, on se rend compte que

$$(\bar{X}+1)^2=\bar{X}^2+2\bar{X}+1=-1+2\bar{X}+1=2\bar{X}.$$

Comme $2^3=1$ dans $\mathbb{F}_7$, et $\bar{X}^4=1$ dans $\mathbb{F}_{49}$, d'après ce qu'on vient de voir, on a

$$(2\bar{X})^{12}=2^{12}\times\bar{X}^{12}=(2^3)^4\times(\bar{X}^4)^3=1$$

dans $\mathbb{F}_{49}$. On en déduit que

$$(\bar{X}+1)^{24}=((\bar{X}+1)^2)^{12}=(2\bar{X})^{12}=1.$$

L'élément $\bar{X}+1$ n'est donc pas générateur de $\mathbb{F}_{49}^\times$ non plus [3].

1. Les autres polynômes unitaires irréductibles de degré 2 sont les 20 polynômes suivants : $X^2+2, X^2-3, X^2\pm X\pm 3, X^2\pm X-1, X^2\pm 2X\pm 2, X^2\pm 2X+3, X^2\pm 3X\pm 1, X^2\pm 3X+5$.

2. maximaux pour la relation d'ordre de divisibilité

3. Il s'ensuit que aucun élément du sous-groupe engendré $\langle\bar{X}+1\rangle$ n'est générateur de $\mathbb{F}_{49}^\times$. Notons que $\bar{X}+1$ est d'ordre 24 car on vient de voir que $(\bar{X}+1)^{24}=1$ et s'il existait un entier naturel non nul $i<24$ tel que $(\bar{X}+1)^i=1$, alors on aurait $(\bar{X}+1)^{12}=1$ ou $(\bar{X}+1)^8=1$, les entiers 8 et 12 étant les diviseurs non triviaux maximaux de 24. Or, comme $(\bar{X}+1)^2=2\bar{X}$, on a

$$(\bar{X}+1)^{12}=(2\bar{X})^6=2^6\times(\bar{X}^2)^3=1\times(-1)^3\neq 1$$

Le calcul précédent [4] pourrait nous donner l'idée de considérer l'élément $\bar{X}-1$ par la suite. On a

$$(\bar{X}-1)^2 = \bar{X}^2 - 2\bar{X} + 1 = -1 - 2\bar{X} + 1 = -2\bar{X}.$$

Bien que cette fois-ci $(-2)^3 = -1 \neq 1$, on a $(-2)^6 = 1$ dans $\mathbb{F}_7$, par conséquence de ce qui précède ou d'après Fermat. On a donc toujours

$$(-2\bar{X})^{12} = (-2)^{12} \times \bar{X}^{12} = ((-2)^6)^2 \times (\bar{X}^4)^3 = 1$$

et encore $(\bar{X}-1)^{24} = 1$. Donc $\bar{X}-1$ n'est pas générateur non plus [5].

Ensuite, considérons l'élément $\bar{X}+2$. On a

$$(\bar{X}+2)^2 = \bar{X}^2 + 4\bar{X} + 4 = -1 - 3\bar{X} + 4 = -3\bar{X} + 3 = -3(\bar{X}-1).$$

En utilisant les calculs ci-dessus, on a donc

$$(\bar{X}+2)^{24} = (-3(\bar{X}-1))^{12} = ((-3)^6)^2 \times ((\bar{X}-1)^2)^6 = \\ 1^2 \times (-2\bar{X})^6 = (-2)^6 \times (\bar{X}^2)^3 = 1 \times (-1)^3 = -1 \neq 1,$$

et

$$(\bar{X}+2)^{16} = (-3(\bar{X}-1))^8 = (-3)^6 \times (-3)^2 \times ((\bar{X}-1)^2)^4 = \\ 1 \times 2 \times (-2\bar{X})^4 = 2 \times 2^4 \times (\bar{X}^2)^2 = 2^{-1} \times (-1)^2 = 4 \neq 1.$$

D'après le c, $\bar{X}+2$ est bien un générateur de $\mathbb{F}_{49}^\times$.

e. D'après le cours, l'ensemble des générateurs de $\mathbb{F}_{49}^\times$ est

$$(\bar{X}+2)^i$$

où $i = 0, \ldots, 47$ avec $\text{pgcd}(i, 48) = 1$, c-à-d, i parcourt les entiers

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47.$$

---

car $2^6 = 1$ dans F_7 d'après Fermat, et

$$(\bar{X}+1)^8 = (2\bar{X})^4 = 2^3 \times 2 \times (\bar{X}^2)^2 = 1 \times 2 \times (-1)^2 = 2 \neq 1.$$

L'élément $\bar{X}+1$ est donc bien d'ordre 24 dans $\mathbb{F}_{49}^\times$. Il s'ensuit que les 24 éléments de $\langle \bar{X}+1 \rangle$ ne sont pas générateurs de $\mathbb{F}_{49}^\times$. Parmi les $48-24=24$ éléments restants de $\mathbb{F}_{49}^\times$ il y en a donc toujours 8 qui ne sont pas générateurs. On ne peut donc pas conclure en choisissant un élément du complémentaire de $\langle \bar{X}+1 \rangle$ dans $\mathbb{F}_{49}^\times$, et on continue la recherche de générateur...

4. mais également le fait que le calcul des puissances 16-ième et 24-ième de $\bar{X}-1$ sont plus simples que celles de $\bar{X}+2$, par exemple

5. On peut encore montrer que $\bar{X}-1$ est d'ordre 24 dans $\mathbb{F}_{49}^\times$, lui aussi. Il engendre donc également un sous-groupe d'ordre 24 dans $\mathbb{F}_{49}^\times$. Comme tout groupe cyclique d'ordre n contient un et un seul sous-groupe d'ordre d, quel que soit d diviseur de n, le sous-groupe engendré $\langle \bar{X}-1 \rangle$ est égal à $\langle \bar{X}+1 \rangle$. Autrement dit, on n'a pas trouvé plus de non générateurs que précédemment, et on continue la recherche...