Sorbonne Université
Année universitaire 2023-2024, Master 1, *Théorie des nombres I* (UE 4MA033).
Corrigé de l'examen partiel du 14 février 2024.

Exercice 1.

(a) Le groupe $(\mathbb{Z}/11\mathbb{Z})^\times$ est de cardinal 10. Modulo 11 on a $2^2 = 4 \neq 1$ et $2^5 = 32 = -1 \neq 1$: l'ordre de 2 dans $(\mathbb{Z}/11\mathbb{Z})^\times$ n'est donc ni 1, ni 2 ;, ni 5 ; par conséquent cet ordre vaut 10 et 2 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^\times$.

(b) Puisque 2 engendre $(\mathbb{Z}/11\mathbb{Z})^\times$ et est d'ordre 10, l'application $\varphi \mapsto \varphi(2)$ induit un isomorphisme de groupes entre $\mathrm{Hom}(\mathbb{Z}/11\mathbb{Z})^\times, \mathbb{C}^\times)$ et le groupe des racines 10-èmes de l'unité dans $\mathbb{C}^\times$. Posons $\xi = \exp(\pi/5)$; c'est une racine primitive 10-ème de l'unité, et il existe donc un unique caractère χ $\mathrm{Hom}(\mathbb{Z}/11\mathbb{Z})^\times$ envoyant 2 sur ξ ; puisque ξ est d'ordre 10, il en va de même de χ.

Pour décrire explicitement χ, nous allons décrire chaque élément de $(\mathbb{Z}/11\mathbb{Z})^\times = \{-5, -4, -3, -2, -1, 1, 2, 3, 4, 5\}$ comme une puissance de 2.

- ◇ $2^0 = 1$;
- ◇ $2^1 = 2$;
- ◇ $2^2 = 4$;
- ◇ $2^3 = 8 = -3$;
- ◇ $2^4 = 2 \cdot (-3) = -6 = 5$;
- ◇ $2^5 = 2 \cdot 5 = 10 = -1$;
- ◇ $2^6 = 2 \cdot (-1) = -2$;
- ◇ $2^7 = 2 \cdot (-2) = -4$;
- ◇ $2^8 = 2 \cdot (-4) = -8 = 3$;
- ◇ $2^9 = 2 \cdot 3 = 6 = -5$.

On peut maintenant dresser la table des valeurs de χ, à l'aide de la formule $\chi(2^n) = \chi(2)^n = \xi^n$; nous simplifierons l'écriture du résultat en nous souvenant que ξ^n ne dépend que de la classe de n modulo 10, et que $xi^5 = -1$. Nous indiquons en noir les éléments de $(\mathbb{Z}/11\mathbb{Z})^\times$, en rouge leur expression comme puissance de 2 et en bleu la valeur prise par χ.

$$\begin{pmatrix} -5 & -4 & -3 & -2 & -1 & 1 & 2 & 3 & 4 & 5 \\ 2^9 & 2^7 & 2^3 & 2^6 & 2^5 & 2^0 & 2^1 & 2^8 & 2^2 & 2^4 \\ \xi^{-1} & \xi^{-3} & \xi^3 & \xi^{-4} & -1 & 1 & \xi & \xi^{-2} & \xi^2 & \xi^4 \end{pmatrix}.$$

Exercice 2. S

(a) Soit $g \in G$ et soient φ et ψ deux caractères de G. On a alors

$$\theta(g)(\varphi\psi) = (\varphi\psi)(g) = \varphi(g)\psi(g) = \theta(g)(\varphi))\theta(g)(\psi)$$

(la première et la troisième égalité proviennent de la définition de $\theta(g)$, et la seconde égalité de la définition de la loi de groupe sur $\widehat{G}$). Par conséquent $\theta(g)$ est un morphisme de groupes de $\widehat{G}$ vers $\mathbb{C}^\times$, c'est-à-dire un élément de $\widehat{\widehat{G}}$.

(b) Soient g et h deux éléments de G et soit $\varphi \in \widehat{G}$. On a

$$\theta(gh)(\varphi) = \varphi(gh) = \varphi(g)\varphi(h) = \theta(g)(\varphi)\theta(h)(\varphi) = (\theta(g)\theta(h))(\varphi)$$

(la première et la troisième égalité proviennent de la définition de θ, la seconde du fait que φ est un caractère, la dernière de la définition de la loi de groupe sur $\widehat{\widehat{G}}$. Par conséquent $\theta(gh) = \theta(g)\theta(h)$ est θ est bien un morphisme de groupes.

(c) On sait d'après le cours que $|\widehat{G}| = |G|$ et $|\widehat{\widehat{G}}| = |\widehat{G}|$. Il vient $|\widehat{\widehat{G}}| = |G|$, et il suffit dès lors de montrer que θ est injective, c'est-à-dire que $\ker \theta = \{e\}$. On procède par contraposition : on se donne un élément $g \neq e$ de G et nous allons montrer que $\theta(g)$ est non trivial. Comme $g \neq e$ l'ordre n de G est strictement supérieur à 1. Le sous-groupe H de G engendré par g est cyclique d'ordre n, et il existe donc un unique morphisme φ de H dans $\mathbb{C}^\times$ envoyant g sur $\exp(2i\pi/n)$, qui est différent de 1 car $n > 1$. Le lemme de prolongement des caractères assure que φ se prolonge en un caractère de G que l'on note encore φ. On a alors

$$\theta(g)(\varphi) = \varphi(g) \neq 1$$

et $\theta(g)$ est en conséquence non trviial.

Exercice 3.

(a) On a $4 \cdot 23 = 92$ si bien que $100 = 8$ modulo 23. Par conséquent on a modulo 23 les égalités $1000 = 10 \cdot 100 = 80 = -12$ puis $2000 = -24 = -1$.

(b) On a dans $\mathbb{Z}[X]$ l'égalité $X^a - 1 = (X-1)(X^{a-1} + X^{a-2} + \ldots + 1)$. En l'évaluant en 2^b on voit que $2^{ab} - 1$ est de la forme $(2^b - 1)m$. Or comme $b \geqslant 2$ on a $2^b - 1 \geqslant 3 > 1$, et comme $a \geqslant 2$ on a $2^{ab} - 1 > 2^b - 1$. Ainsi $2^{ab} - 1$ possède-t-il un diviseur strictement compris entre 1 et $2^{ab} - 1$, à savoir $2^b - 1$; il n'est donc pas premier.

(c) Si l'entier n s'écrit comme produit de deux entiers au moins égal à 2, c'est-à-dire encore si $n > 1$ et n n'est pas premier, alors 2^n n'est pas premier par ce qui précède. Et par ailleurs $2^1 - 1 = 1$ qui n'est pas premier. Pour que $2^n - 1$ soit premier, il est donc nécessaire que n soit premier.

(d) Testons la primalité de $2^p - 1$ pour différentes valeurs premières de p.
   - $2^2 - 1 = 3$, qui est premier :
   - $2^3 - 1 = 7$, qui est premier.
   - $2^5 - 1 = 31$, qui est premier.
   - $2^7 - 1 = 127$, qui est également premier : en effet il n'est pas divisible par 2 ni 5, il n'est pas divisible par 3 car $1 + 2 + 7 = 10 \neq 0$ modulo 3, il n'est pas divisible par 7 car $127 = 140 - 13 = 1$ modulo 7, et il n'est pas divisible par 11 car $7 - 2 + 1 = 6 \neq 0$ modulo 11, et on peut s'arrêter là car $13^2 = 169 > 127$;
   - $2^{11} - 1 = 2047$ (pour calculer 2^{11} on peut se rappeler que $2^{10} = 1024$, c'est une valeur qu'il est bon d'avoir comme point de repère) ; et $2047 = 2000 + 47 = -1 + 47 = 46 = 0$ modulo 23 (la deuxième égalité provient de la question (a)) ; par conséquent 2047 n'est pas premier, et l'on tient notre contre-exemple.

Exercice 4.

(a) Comme a est impair on a dans $\mathbb{Z}[X]$ l'égalité $X^a+1=(X+1)(X^{a-1}-X^{a-2}+\ldots+(-1)^iX^i+\ldots+1)$. En l'évaluant en 2^b on voit que $2^{ab}+1$ est de la forme $(2^b+1)m$. Or $2^b+1>1$, et $2^b+12<2^{ab}+1$ car $a>1$. Ainsi $2^{ab}+1$ possède-t-il un diviseur strictement compris entre 1 et $2^{ab}+1$, à savoir 2^b+1 ; il n'est donc pas premier.

(b) Si 2^{m+1} est premier il résulte de la question précédente que m ne peut pas avoir de diviseur premier impair, si bien que m est une puissance de 2.

Erratum. Je réalise en tapant la correction qu'il fallait imposer $m>0$: l'argument donné suppose implicitement qu'on est dans ce cas, et 2^0+1 est égal à 2, donc est premier.

(c) On a $F_n=2^{2^n}+1=0$ modulo p, donc $2^{2^{n+1}}$ est égal à (-1) modulo p. Par conséquent, $2^{2^{n+1}}=(-1)^2=1$ modulo p. L'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$ divise donc 2^{n+1}, ce qui veut dire qu'il est de la forme 2^r avec $r\leqslant n+1$. Mais si l'on avait $r\leqslant n$ alors 2^r diviserait 2^n et l'on aurait alors $2^n=1$ modulo p, ce qui est absurde (notez que F_n est impair, donc p aussi, et (-1) est dès lors différent de 1 modulo p !). Par conséquent, l'ordre de multiplicatif de 2 modulo p est exactement 2^{n+1}.

Puisque $(\mathbb{Z}/p\mathbb{Z})^\times$ est de cardinal $p-1$, cet ordre divise $p-1$. Il existe donc un entier k tel que $p-1=k\cdot 2^{n+1}$, c'est-à-dire encore $p=k\cdot 2^{n+1}+1$.

(d)
- ◇ $F_0=2^{2^0}+1=2+1=3$, qui est premier ;
- ◇ $F_1=2^{2^1}+1=2^2+1=5$, qui est premier ;
- ◇ $F_2=2^{2^2}+1=2^4+1=17$, qui est premier ;
- ◇ $F_3=2^{2^3}+1=16^2+1=257$, dont nous allons vérifier qu'il est premier ; il est clair que 257 n'est divisible ni par 2 ni par 5 ; il n'est pas divisible par 3 (car $7+5+2=2$ modulo 3) ; il n'est pas divisible par 7 car $257=210+47=47=-2$ modulo 7 ; il n'est pas divisible par 11 car $7-2+5=-1$ modulo 11, et il n'est pas divisible par 13 car $257=260-3=-3$ modulo 13 ; et l'on peut s'arrêter là puisque $17^2=289>257$.

(e)(e1) On sait d'après la question (c) que tout diviseur premier p de F_4 sera de la forme $k\cdot 2^5+1=32k+1$. Pour montrer que F_4 est premier il suffit de s'assurer qu'il ne possède aucun diviseur premier $\leqslant\sqrt{F_4}$; compte-tenu de ce qui précède, il suffit donc de s'assurer que pour tout nombre premier p de la forme $32k+1$ tel que $p^2<F_4$, l'entier p ne divise pas F_4. Or comme $32\cdot 8+1=257=(256+1)^2$ on a $(32\cdot 8+1)^2>256^2+1=F_4$; il suffit donc de considérer les nombres premiers de la forme $32k+1$ avec $k\leqslant 7$.

(e2) On procède par inspection en faisant varier k de 1 à 7.
- ◇ $32\cdot 1+1=33$, qui n'est pas premier ;
- ◇ $32\cdot 2+1=65$ qui n'est pas premier (c'est $13\cdot 5$) ;
- ◇ $32\cdot 3+1=97$, qui est premier : il n'est en effet multiple ni de 2 ni de 5, il n'est pas multiple de 3 puisque $9+7=1$ modulo 3, et il n'est pas multiple de 7 (le dernier diviseur premier à considérer puisque $11^2=121$) car $97=70+27=-1$ modulo 7 ;
- ◇ $32\cdot 4+1=129$ qui n'est pas premier car il est multiple de 3, puisque $1+2+9$ est nul modulo 3 ;

- $\diamond$ $32 \cdot 5 + 1 = 161$ qui n'est pas premier car $161 = 140 + 21 = 0$ modulo 7 ;
- $\diamond$ $32 \cdot 6 + 1 = 193$, qui est premier : en effet 193 n'est multiple ni de 2 ni de 5, il n'est pas multiple de 3 car $1 + 9 + 3 = 1$ modulo 3, il n'est pas multiple de 7 car $193 = 210 - 17 = -17 = 4$ modulo 7, il n'est pas multiple de 11 car $3 - 9 + 1 = -5$ modulo 11, et il n'est pas multiple de 13 car $193 = 130 + 63 = 65 - 2 = -2$ modulo 13 (et $17^2 = 289 > 193$).
- $\diamond$ $32 \cdot 7 + 1 = 225$ qui est multiple de 5 et n'est donc pas premier.

(e3) Nous allons montrer que $2^{16} \neq (-1)$ modulo 97 aussi bien que modulo 193. Nous calculerons dans les deux cas 2^{16} par élévations au carré successives.

- $\diamond$ Nous travaillons modulo 97. Nous allons calculer 2^{16} en remarquant que $100 = 3$. On a $2^2 = 4$, et $2^4 = 4^2 = 16$. On a alors $2^8 = (16)^2 = 256 = 2 \cdot 3 + 56 = 62 = -35$, et

$$2^{16} = (-35)^2 = 900 + 300 + 25 = 3 \cdot 12 + 25 = 61 \neq (-1).$$

- $\diamond$ Nous travaillons modulo 193. Nous allons calculer 2^{16} en remarquant que $200 = 7$. On a $2^2 = 4$, et $2^4 = 4^2 = 16$. On a alors $2^8 = (16)^2 = 256 = 7 + 56 = 63$, et

$$2^{16} = (63)^2 = 3600 + 360 + 9 = 3800 + 169 = 7 \cdot 19 + 169$$

$$= 133 + 169 = 7 + 33 + 69 = 109 \neq (-1).$$

(f) On travaille modulo 641. Les égalités $641 = 640 + 1 = 625 + 16$ peuvent se récrire $64 \cdot 10 + 1 = 2^7 \cdot 5 + 1 = 0$ et $5^4 + 2^4 = 0$. On a donc $2^7 \cdot 5 = -1$; en élevant cette égalité à la puissance 4 on obtient $2^{28} \cdot 5^4 = 1$. En utilisant le fait que $5^4 = -2^4$ on en déduit que $-2^{32} = 1$, donc que $2^{32} + 1 = 0$, ce qu'il fallait démontrer.

Le nombre $F_5 = 2^{32} + 1$ est donc divisible par 641. Comme il est évidemment strictement supérieur à 641 (on a $2^{10} = 1024$, si bien que $2^{30} > 10^9$ et $2^{32} > 4 \cdot 10^9$), il n'est pas premier.

Exercice 5.

(a)

(a1) Si G est un groupe fini l'ordre de tout élément de G divise $|G|$, et lorsque G est cyclique la réciproque est vraie : tout diviseur d de $|G|$ est l'ordre d'un élément de G (c'est supposé connu ; si vous voulez une justification, remarquez que pour tout $n > 0$ et tout diviseur d de n la classe de n/d est d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$). Par conséquent un groupe cyclique G possède un élément d'ordre 3 si et seulement si 3 divise $|G|$.

(a2) On sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique de cardinal $p - 1$. Il possède donc par ce qui précède un élément d'ordre 3 si et seulement si 3 divise $p - 1$, c'est-à-dire encore si et seulement si p est égal à 1 modulo 3. un élément d'ordre 3.

(b) *Seconde méthode : par les équations quadratiques.*

(b1) Comme p est impair $1/2$ existe dans $\mathbb{Z}/p\mathbb{Z}$. On a alors

$$X^2 + aX + b = (X + a/2)^2 + b - a^2/4.$$

Le polynôme étudié a donc une racine dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $a^2/4 - b$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$. Comme 4 est un carré non nul de $\mathbb{Z}/p\mathbb{Z}$, cela revient à demander que $4(a^2/4-b) = a^2-4b$ soit un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Supposons que ce soit le cas et notons $\sqrt{a^2-4b}$ l'une des deux racines carrées de $a^2 - 4b$ dans $\mathbb{Z}/p\mathbb{Z}$; l'autre est alors $-\sqrt{a^2-4b}$. Les racines de $X^2 + aX + b$ sont les solutions de l'équation

$$(X + a/2)^2 = a^2/4 - b,$$

à savoir

$$\frac{-a+\sqrt{a^2-4b}}{2} \quad \text{et} \quad \frac{-a-\sqrt{a^2-4b}}{2}.$$

Donnons maintenant un contre-exemple dans le cas où $p = 2$. Le polynôme $X^2 + X + 1$ n'a pas de racine dans $\mathbb{Z}/2\mathbb{Z}$ (il vaut 1 en 0 et en 1). Et pourtant $1^2 - 4 \cdot 1 = 1$ est un carré dans $\mathbb{Z}/2\mathbb{Z}$.

(b2) Soit a un élément de $\mathbb{Z}/p\mathbb{Z}$. C'est une racine cubique primitive de l'unité si et seulement si $a^3 = 1$ (ce qui force a à être non nul et d'ordre multiplicatif divisant 3, donc valant 1 ou 3) et $a \neq 1$. Notons par ailleurs qu'on a $a^3 - 1 = (a-1)(a^2 + a + 1)$.

Supposons que a soit une racine cubique primitive de l'unité. Comme $a^3 = 1$ on a $(a-1)(a^2+a+1) = 0$ et comme $a \neq 1$ il vient $a^2 + a + 1 = 0$.

Réciproquement supposons que $a^2 + a + 1$ est nul. On a alors $a^3-1 = (a-1)(a^2+a+1) = 0$, et de plus $a \neq 1$ car $1^2+1+1 = 3 \neq 0$ puisque $p \neq 3$.

On a donc bien l'équivalence requise.

(b3) Soit p un nombre premier. Si $p = 2$ alors p vaut (-1) modulo 3 et $(\mathbb{Z}/p\mathbb{Z})^\times$ est égal à $\{1\}$ et n'a pas d'élément d'ordre 3. Si $p = 3$ alors p est nul modulo 3 et $(\mathbb{Z}/p\mathbb{Z})^\times$ est égal à $\{-1, 1\}$ et n'a pas d'élément d'ordre 3.

Supposons $p > 3$. D'après (b2), $\mathbb{Z}/p\mathbb{Z}$ possède une racine primitive cubique de l'unité si et seulement si $X^2 + X + 1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$. En vertu de (b1) cela revient à demander que $1^2 - 4 = (-3)$ soit un carré modulo p, c'est à dire que $\left(\frac{-3}{p}\right) = 1$.

Or on a

$$\begin{aligned}
\left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\
&= \left(\frac{-1}{p}\right)(-1)^{\frac{p(p-1)}{2}\cdot\frac{2}{2}}\left(\frac{p}{3}\right) \\
&= \left(\frac{-1}{p}\right)^2\left(\frac{p}{3}\right) \\
&= \left(\frac{p}{3}\right)
\end{aligned}$$

(la seconde égalité provient de la loi de réciprocité quadratique).

Par conséquent $\mathbb{Z}/p\mathbb{Z}$ possède une racine cubique primitive de l'unité si et seulement si p est un carré modulo 3, ce qui revient à demander que $p = 1$ modulo 3 puisque $(\mathbb{Z}/3\mathbb{Z})^\times = \{-1, 1\}$.

On retrouve donc bien les conditions mises en évidence à la partie (a).