MT10

Simon Chabot

Aucune garantie d'exactitude
mais, j'espère que ça l'est =)

1 Structures

1.1 Monoïdes

Définition 1.1 (Monoïde) *$(M, \star, e)$ tel que $\star$ soit associative et que e soit élément neutre.*

Proposition 1.1 (Sous-Monoïde) *$N \subset M$. $(N, \star, e)$ est un sous-monoïde si et seulement si :*

$$\begin{cases} e \in N \\ \forall x, x' \in N, x \star x' \in N \end{cases}$$

1.2 Groupe

Définition 1.2 (Groupe) *$(G, \star, e)$ tel que se soit un monoïde et que tout élément de G admette un symétrique.*

Proposition 1.2 (Sous groupe) *$H \subset G$. $(G, \star, e)$ est un sous-groupe de G si et seulement si*

$$\begin{cases} H \neq \emptyset \\ x, y \in H \Rightarrow x \star y^{-1} \in H \end{cases}$$

Définition 1.3 (Ordre et indice) *Soit G un groupe et H un sous-groupe de G.*

1. **a.** *Pour un groupe* $\operatorname{ord} G = \operatorname{card} G$
   b. *Soit* $a \in G$, $\operatorname{ord} a = \min\{n \in \mathbb{N}, a^n = e\}$
2. *L'*indice *de H de G est le nombre de classe d'équivalence de $\mathcal{R}_g$ (ou de $\mathcal{R}_d$) associée à H et notée $[G : H]$.*

Théorème 1.1 (Lagrange)

$$\operatorname{ord} G = [G : H] \operatorname{ord} H$$

Preuve. *G est la réunion disjointe des $[G : H]$ classes d'équivalences de $\mathcal{R}_g$, qui ont chacune* $\operatorname{ord} H$ *éléments. (autre preuve avec une bijection entre les éléments de chaque classe et H, et comme le cardinal est fini, on abouti au fait que chaque classe a le même nombre d'éléments, ce qui permet de conclure.)*

Définition 1.4 (Sous groupe distingué) *Soit $H \subset G$.*

$$H \lhd G \Leftrightarrow (\forall x \in G, \forall h \in H), x \star h \star x^{-1} \in H$$

Ou de manière équivalente[1] *:*
– $\forall x \in G, xHx^{-1} \subset H$
– $\forall x \in G, xH = Hx$

Preuve.

$$\begin{aligned} x \star h \star x^{-1} \in H & \Leftrightarrow \\ x \star h \in Hx & \Leftrightarrow \\ xH \subset Hx & \end{aligned}$$

De la même façon, on trouve $Hx \subset xH$, d'où $xH = Hx$

Théorème 1.2 *Un groupe commutatif a tous ses sous-groupes distingués.*
La réciproque est fausse (contre exemple : groupe des quaternions $\mathbb{H}_8$).

Définition 1.5 (Sous groupe engendré) *$< A >$ est le plus petit sous-groupe de G contenant A.*

$$< A >= \left\{ \prod_{k=1}^{n} x_k, n \in \mathbb{N}, x_k \in A \text{ ou } x_k^{-1} \in A \right\}$$

Définition 1.6 (Morphisme de groupes) *Soit $f : G \to G'$ un morphisme de groupes (ie $f(x \star y) = f(x) \star' f(y)$).*

1. *f injectif* ssi $\forall x, y \in G, \quad (f(x) = f(y)) \Rightarrow (x = y)$ ssi $\ker f = \{e\}$
2. *f surjectif* ssi $\forall y \in G', \exists x \in G \quad f(x) = y$ ssi $\operatorname{Im} f = G'$

1.3 Action de groupe et orbite

Définition 1.7 (Action de groupe) *On appelle* action *d'un groupe G sur l'ensemble X une application telle que :*

$$\begin{aligned} \phi : G \times X &\to X \\ (g, x) &\mapsto \phi(g, x) \end{aligned}$$

1. $\forall x \in X, \quad \phi(e, x) = x$
2. $\forall x \in X, \forall g, g' \in G, \quad \phi(g', \phi(g, x)) = \phi(g' \star g, x)$

Définition 1.8 (Orbite) *On appelle* orbite *de $x \in X$ sous l'action de G :*

$$\operatorname{Orb} x = \{g \star x, g \in G\} \subset X$$

Proposition 1.3 *Les orbites forment une partition de X. Elles sont les classes d'équivalence de la relation*

$$\forall x, x' \in X \quad xSx' \Leftrightarrow (\exists g \in G : x' = g \star x)$$

1. On a la notation suivante : $Hx = \{y \star x : y \in H\}$ et $xH = \{x \star y : y \in H\}$

1.4 Anneau

Définition 1.9 (Anneau) $(A, +, 0, \star, 1)$ *est un anneau si :*

1. $(A, +, 0)$ *un groupe abélien*[2]
2. $(A, \star, 1)$ *un monoïde*
3. $\star$ *distributive par rapport à* $+$ *(ie* $\forall a, b, c \in A, a \star (b + c) = a \star b + a \star c$ *et* $(a + b) \star c = a \star c + a \star b$*).*

Définition 1.10 (Morphisme d'anneaux) *Soit* A *et* A' *deux anneaux. Une application* $f : A \to A'$ *est un morphisme d'anneau si :*

1. $\forall x_1, x_2 \in A \quad f(x_1 + x_2) = f(x_1) +' f(x_2)$
2. $f(e) = e'$
3. $\forall x_1, x_2 \in A \quad f(x_1 \star x_2) = f(x_1) \star' f(x_2)$

Définition 1.11 (*A*-algèbre) *Une* A-algèbre *est un couple* (B, j) *où* B *est un anneau et* $j : A \to B$ *un morphisme d'anneau.*

Si j *est injective, on dit que* (B, j) *est une* extension d'anneau *et on note* $A \hookrightarrow^j B$.

Définition 1.12 (Idéal) *On dit que* $I \subset A$ *est un* idéal *si :*

1. I *est un sous-groupe de* $(A, +, 0)$
2. $\forall x \in A \quad xI \subset I$ *et* $Ix \subset I$

Exemple 1.1 (et remarques)
- *Les idéaux de* Z *sont ses sous-groupes* $n\mathbb{Z}$.
- *Soit* I *un idéal de* A. I *contient un élément inversible de* A ssi $I = A$ ssi $1 \in I$.
- *On appelle* Idéal propre *un idéal différent de* A.
- *Les seuls idéaux d'un corps commutatifs sont les idéaux triviaux (ie* A *et* $\{0\}$ *à cause de la commutativité).*

Définition 1.13 (Anneau intègre) *Un anneau est dit* intègre ssi *:*

$$\forall x, y \in A \quad (x \star y = 0) \Rightarrow (x = 0) \text{ ou } (y = 0)$$

Définition 1.14 (Idéal premier) *On dit que* I *est un idéal premier* ssi A/I *est intègre* ssi *:*

$$\begin{cases} I \neq A \\ \forall x, y \in A \quad x \star y \in I \Rightarrow (x \in I \text{ ou } y \in I) \end{cases}$$

Définition 1.15 (Idéal maximal) *On dit que* I *est un idéal maximal* ssi A/I *est commutatif* ssi *il n'existe que deux idéaux contenant* I *(c'est à dire* A *et* I*).*

Définition 1.16 (Idéal principal) *On dit que* I *est un idéal principal* ssi *il n'est engendré que par un seul élément de* A.

à gauche I *est dit principal à gauche s'il existe un élément* a *de* I *tel que, pour tout* $x \in I$*, il existe un élément* y *de* A *tel que* $x = y \star a$*. On note* $I = Aa$.

à droite *idem mais à droite (ie* $x = a \star y$*, et noté* $I = aA$*).*

Si I *est principal à droite et à gauche, on notera* $I = (a)$*, qui est le plus petit idéal contenant* a.

Proposition 1.4 *Soit* A *un anneau* commutatif *et* intègre. *Soit* $a \in A, a \neq 0$. *Alors* (a) *est* premier *si et seulement* a *est* premier.

2. ie : commutatif

1.5 Corps

Définition 1.17 (Corps) $(E, +, 0, \star, 1)$ *est un corps si :*

1. $(E, +, 0, \star, 1)$ *est un anneau*
2. $(E \backslash \{0\}, \star, 1)$ *est un groupe*

Définition 1.18 (Caractéristique) *On appelle* caractéristique *d'un anneau* A *l'ordre pour la loi additive de l'élément neutre de la loi multiplicative, si cet ordre est fini. C'est a dire :*

$$n \star 1_A = \underbrace{1_A + 1_A + \ldots + 1_A}_{n \text{ fois}} = 0$$

où n *est le plus petit possible et non-nul. Si un tel entier n'existe pas (ie est infini) on dit que* A *est de caractéristique nulle.*

Proposition 1.5
1. *La caractéristique* c *d'un anneau* A *est l'*unique *entier* $c \in \mathbb{N}$ *tel que* $\mathbb{Z}/c\mathbb{Z}$ *soit un sous-anneau de* A.
2. *La caractéristique* c *d'un anneau* A intègre *est soit nulle, soit un nombre premier.*
3. *Tout corps* fini *a pour caractéristique un nombre premier* p *et pour cardinal une puissance de ce nombre.*

1.6 Relations

Une relation S sur un ensemble A est un sous-ensemble du produit cartésien $A \times A$. Si $(x, y) \in S$, on notera xSy.

1.6.1 D'équivalence

Définition 1.19 (Relation d'équivalence) *Une relation* S *sur* A *est dite d'équivalence si pour tout* $x, y, z \in A$ *on a :*

Réflexivité xSx

Symétrie $xSy \Rightarrow ySx$

Transitivité $(xSy \wedge ySz) \Rightarrow xSz$

1.6.2 D'ordre

Définition 1.20 (Relation d'ordre) *Une relation* S *sur* A *est dite d'ordre si pour tout* $x, y, z \in A$ *on a :*

Réflexivité xSx

Anti-symétrie $(xSy \wedge ySx) \Rightarrow (x = y)$

Transitivité $(xSy \wedge ySz) \Rightarrow xSz$

1.6.3 Compatibilité

Définition 1.21 (Compatibilité) *Soit un ensemble* E *muni d'une loi de composition interne* $\sim$*. On dit que la relation* S *est compatible avec la loi* $\sim$ *si :*

$$\forall (x, x', y, y') \in E^4, \quad (xSy \text{ et } x'Sy') \Rightarrow (x \sim x')S(y \sim y')$$

2 Arithmétique

Théorème 2.1 (TFA)

$$\forall n \in \mathbb{N}\backslash\{0\}, n = \prod_{p\in\mathbb{P}} p^{v_p(n)}$$

1. $a|b \Leftrightarrow (\forall p \in \mathbb{P}, v_p(a) \leqslant v_p(b))$
2. (Lemme d'Euclide) $(p \in \mathbb{P}$ et $p|ab) \Rightarrow (p|a$ ou $p|b)$
3. (Lemme de Gauss) $(c|ab$ et $c \wedge a = 1) \Rightarrow c|b$

Théorème 2.2 (petit théorème de Fermat) *Soient $p \in \mathbb{P}$ et $a \in \mathbb{N}$.*

$$a \wedge p = 1 \Rightarrow a^{p-1} = 1[p]$$

Théorème 2.3 (d'Euler) *Soient $n \in \mathbb{N}, n \leqslant 2$ et $a \in \mathbb{N}$.*

$$a \wedge n = 1 \Rightarrow a^{\phi(n)} = 1[n]$$

Définition 2.1 (pseudo-premier en base *a*) *On dit qu'un entier n est* pseudo-premier en base a *si :*

$$a \wedge n = 1 \text{ et } a^{n-1} = 1[n]$$

Proposition 2.1 *Un nombre premier p est pseudo-premier en tout base a telle que $a \wedge p = 1$*
La réciproque est fausse ! Il existe des nombres n premiers en tout base a telle que $a \wedge n = 1$ et qui ne sont pas premiers. Ce sont les nombres de Carmichael *(ex : $561 = 3 \times 11 \times 17$)*

2.1 PGCD, PPCM et sous-groupe

Définition 2.2 (pcgd, ppcm)
1. $b|a \Leftrightarrow a\mathbb{Z} \subset b\mathbb{Z}$
2. $d = a \wedge b \Leftrightarrow d \in \mathbb{N}, a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ *(D'où Bézout)*
3. $m = a \vee b \Leftrightarrow m \in \mathbb{N}, a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$

2.2 Les inversibles de $\mathbb{Z}/n\mathbb{Z}$

1. $a \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $a \wedge n = 1$

$$\begin{aligned} aa' = 1 &\Leftrightarrow aa' = 1[n] \Leftrightarrow aa' - 1 = kn \\ &\Leftrightarrow aa' - kn = 1 \Leftrightarrow a \wedge n = 1 \end{aligned}$$

2. Indicatrice d'Euler : $\phi(1) = 1$. Puis, pour tout $n \geqslant 2$:

$$\begin{aligned} \phi(n) &= \text{card}(\mathbb{Z}/n\mathbb{Z})^\star \\ &= \text{card}\left\{x \in [0; n-1], x \wedge n = 1\right\} \end{aligned}$$

$$\begin{aligned} p \in \mathbb{P}, \phi(p^\alpha) &= (p-1)p^{\alpha-1} \\ m \wedge n = 1 &\Rightarrow \phi(mn) = \phi(m)\phi(n) \\ \phi(n) &= \prod_{p\in\mathbb{P}} (p-1)p^{v_p(n)-1} \end{aligned}$$

3. Formule d'Euler :

$$n = \sum_{d|n} \phi(d)$$

2.3 Théorème des restes chinois

Théorème 2.4 (des restes chinois) *Soient $n_1, \ldots, n_k$ des entiers deux à deux premiers entre eux. Il existe un unique entier x modulo $n = \prod n_i$ tel que :*

$$\begin{cases} x & \equiv a_1 \mod n_1 \\ & \ldots \\ x & \equiv a_k \mod n_k \end{cases}$$

Preuve. Pour chaque i, n_i et $\hat{n_i} = \frac{n}{n_i}$ sont premiers entre eux. D'après Bezout-Bachet, il existe u_i et v_i tels que $u_i n_i + v_i \hat{n_i} = 1$. On pose $e_i = v_i \hat{n_i}$ (et donc $e_i \equiv 1[n_i]$ et $e_i \equiv 0[n_j], j \neq i$). Une solution particulière est donc $x = \sum_{i=1}^k a_i e_i$.

2.4 Quelques résultats à l'arrache servant d'exemples

1. 2 est inversible dans $\mathbb{Z}/27\mathbb{Z}$ et son inverse est 14.

   Preuve. $2 \wedge 27 = 1$ donc admet un inverse. On applique l'algorithme d'Euclide et on trouve $27 = 2 * 13 + 1$ d'où $2 * (-13) = 1[27]$. Donc $2^{-1} = -13 = 14$.

2. 12^{2011} multiple de 11 ? Non.

   Preuve. car $12 = 1[11]$, donc $12^{2011} = 1[11]$.

3. $3^{2n} - 2^n$ est-il multiple de 7 pour tout $n \in \mathbb{N}$. Oui.

   Preuve. Calculons modulo 7.

$$3^{2n} - 2^n = 9^n - 2^n = 2^n - 2^n = 0$$

4. Reste de la division euclidienne de 65^n par 9 ?

   Preuve.

$$\begin{aligned} 65 &= 2[9] & 65^2 &= 4[9] \\ 65^3 &= 8[9] & 65^4 &= 7[9] \\ 65^5 &= 5[9] & 65^6 &= 1[9] \end{aligned}$$

   d'où :

$$\begin{aligned} 65^{6k} &= 1[9] & 65^{6k+1} &= 2[9] \\ 65^{6k+2} &= 4[9] & 65^{6k+3} &= 8[9] \\ 65^{6k+4} &= 7[9] & 65^{6k+5} &= 5[9] \end{aligned}$$

3 Corps finis

Théorème 3.1 *Soit $q = p^n, n \in \mathbb{N}, p \in \mathbb{P}$. alors on a :*

$$X^q - X = \prod_{\substack{P \in \mathbb{F}_p[X] \\ \text{irréduc, unitaire} \\ \deg P | n}} P(X)$$

Théorème 3.2 *Le nombre de générateurs d'un groupe cyclique d'ordre n est égal à $\phi(n)$*

Définition 3.1 (Élément primitif) *On appelle* élément primitif *de K un générateur de K^*.*

Théorème 3.3 *Si K est un corps fini, alors le groupe multiplicatif K^* est cyclique.*

Proposition 3.1 (Nombres de polynômes irréductibles) *Soit $N(d)$ le nombre de polynômes irréductibles et unitaire de degré d dans $\mathbb{F}_q[X]$. On a :*

$$N(d) = \frac{1}{d} \sum_{n|d} \mu\left(\frac{d}{n}\right) q^n$$

où, $\mu(1) = 1$, et $\forall n \in \mathbb{N}, n > 1$,

$$\mu(n) = \begin{cases} 0 & \text{Si } n \text{ contient un facteur carré} \\ (-1)^s & \text{Si } n = p_1 \dots p_s, \text{ produit de premiers sans répétition} \end{cases}$$

Définition 3.2 (Endomorphisme de Frobenius) *Soit A un anneau commutatif unitaire ayant pour caractéristique $p \in \mathbb{P}$. L'*endormorphisme de Frobenius *est l'application définie par :*

$$\begin{aligned} Frob_A : A &\to A \\ x &\mapsto x^p \end{aligned}$$

Proposition 3.2 *On a :*

1. $\forall a, b \in A, Frob_A(ab) = Frob_A(a) Frob_A(b)$
2. $\forall a, b \in A, Frob_A(a + b) = Frob_A(a) + Frob_A(b)$
3. $\forall a \in A, Frob_A(a^{-1}) = Frob_A(a)^{-1}$
4. $\forall a \in A, Frob_A(-a) = -Frob_A(a)$
5. *Si A est intègre, $Frob_A$ est injectif.*
6. *Si A est intègre et fini, $Frob_A$ est bijectif.*
7. *Tout corps premier est invariant par Frobenius.*
8. $\forall P[X] \in \mathbb{F}_q[X], P[X^p] = P[X]^p$

4 Courbes elliptiques

Définition 4.1 *Les courbes elliptiques sous la forme de Weierstrass réduite sont de la forme :*

$$y^2 = x^3 + px + q$$

Proposition 4.1 (Règles de calculs) *Soient $P_1(x_1, y_1)$ et $P_2(x_2, y_2)$ deux points de la courbe elliptique E.*

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{si } P_1 \neq P_2 \\ \frac{3x_1^2 + p}{2y_1} & \text{sinon} \end{cases}$$

On a $P_3 = P_1 + P_2$ tel que :

$$\begin{cases} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \end{cases}$$

5 Primalité et factorisation

5.1 Test de Miller-Rabin

Basé sur deux propriétés des nombres premiers :

1. $\forall a \in \mathbb{N} \setminus \{0\}, a^{p-1} = 1[p]$ (théorème de Fermat)
2. Dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^2 = 1$ n'a que deux solutions : $x = 1$ et $x = -1 = p - 1$.

On écrit $n - 1$ sous la forme $n - 1 = 2^s t$, où t est impair. On choisit au hasard un entier b dans l'intervalle $[\![1; n-1]\!]$ et on calcul les résidus dans $[\![0; n-1]\!]$ des puissances suivantes de b, modulo n :

$$b^t[n], b^{2t}[n], b^{4t}[n], \dots, b^{2^{s-1}t}[n], b^{n-1}[n] \tag{1}$$

On dit que n passe le test de primalité de Miller-Rabin en base b si les deux résultats suivants sont vérifiés :

1. $b^{n-1} = 1[n]$
2. Si le premier élément de (1) n'est pas égal à 1 et que si $b^{2^r t}[n]$ est le premier élément égal à 1, alors l'élément précédent $b^{2^{r-1}t}[n]$ est égal à $n - 1$

5.2 Factorisation par la méthode $p - 1$-Pollard

Définition 5.1 (B-Smooth) *Un entier n est dit* B-Smooth *si et seulement si tous ses facteurs sont inférieurs ou égaux à B.*

Définition 5.2 (B-Supersmooth) *Un entier n est dit* B-Supersmooth *si et seulement si toutes les puissances de nombres premiers qui le divisent sont inférieurs ou égales à B.*

Exemple 5.1 *$72 = 2^3 \times 3^2$ est 3-smooth et 9-supersmooth.*

Soit N un entier à factoriser. On choisit B et on suppose qu'un facteur premier p de N est tel que $p - 1$ soit B-supersmooth. Nous cherchons donc p. Soit a, pris au hasard dans $[\![2; n-2]\!]$. Si a n'est pas divisible par p, alors on a

$$a^{p-1} = 1[p]$$

On pose $m = \text{lcm}(1, 2, \dots, B)$. Ainsi, $p - 1 | m$, d'où $a^m = 1[p]$. Si $1 < \gcd(a^m - 1, N) < N$, alors $\gcd(a^m - 1, N)$ est un facteur non trivial de N. Sinon, il faut changer de B et de a.

6 Quelques tables multiplicatives

	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

TABLE 1: $\mathbf{F}_4 \simeq \mathbf{F}_2/(X^2+X+1)$

	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

TABLE 2: $\mathbf{F}_8 \simeq \mathbf{F}_2/(X^3+X+1)$

	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	1	$\alpha+1$
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	1	α	$\alpha^2+\alpha+1$	α^2
α^2	0	α^2	α^2+1	1	$\alpha^2+\alpha+1$	$\alpha+1$	α	$\alpha^2+\alpha$
α^2+1	0	α^2+1	$\alpha^2+\alpha+1$	α	$\alpha+1$	$\alpha^2+\alpha$	α^2	1
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	1	$\alpha^2+\alpha+1$	α	α^2	$\alpha+1$	α^2+1
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	$\alpha+1$	α^2	$\alpha^2+\alpha$	1	α^2+1	α

TABLE 3: $\mathbf{F}_8 \simeq \mathbf{F}_2/(X^3+X^2+1)$

	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	2	$\alpha+2$	$2\alpha+2$	1	$\alpha+1$	$2\alpha+1$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$\alpha+2$	2α	1	$2\alpha+1$	2	α
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	1	α	$\alpha+1$	2α	2
2α	0	2α	α	1	$2\alpha+1$	$\alpha+1$	2	$2\alpha+2$	$\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$\alpha+1$	2	2α	$2\alpha+2$	α	1
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$2\alpha+1$	α	2	$\alpha+2$	1	2α

TABLE 4: $\mathbf{F}_9 \simeq \mathbf{F}_3/(X^2+1)$

	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	$2\alpha+1$	1	$\alpha+1$	$\alpha+2$	$2\alpha+2$	2
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	1	$\alpha+2$	2α	2	α	$2\alpha+1$
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$\alpha+1$	2α	2	$2\alpha+2$	1	α
2α	0	2α	α	$\alpha+2$	2	$2\alpha+2$	$2\alpha+1$	$\alpha+1$	1
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$2\alpha+2$	α	1	$\alpha+1$	2	2α
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	2	$2\alpha+1$	α	1	2α	$\alpha+2$

TABLE 5: $\mathbf{F}_9 \simeq \mathbf{F}_3/(X^2+X+2)$

	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	$\alpha+1$	$2\alpha+1$	1	$2\alpha+2$	2	$\alpha+2$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$2\alpha+1$	2	α	$\alpha+2$	2α	1
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	1	α	$2\alpha+2$	2	$\alpha+1$	2α
2α	0	2α	α	$2\alpha+2$	$\alpha+2$	2	$\alpha+1$	1	$2\alpha+1$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	2	2α	$\alpha+1$	1	$2\alpha+2$	α
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$\alpha+2$	1	2α	$2\alpha+1$	α	2

TABLE 6: $\mathbf{F}_9 \simeq \mathbf{F}_3/(X^2+2X+2)$