EPFL - Printemps 2023 — Prof. Zs. Patakfalvi
Anneaux et Corps — **Exercices**
Solutions 5

Exercice 1. (a) Notons tout d'abord qu'un élément de $x \in k[t]/t^2$ s'écrit uniquement sous la forme $x = \lambda + \mu t$ avec $\lambda, \mu \in k$. Notons aussi qu'un élément est inversible si et seulement si $\lambda \neq 0$. En effet si $\lambda = 0$, on a que x est nilpotent, et si $\lambda \neq 0$, on a $x^{-1} = \lambda^{-1}(1 - \mu\lambda^{-1}t)$. Autrement dit on a $(t) = (k[t]/t^2) \setminus (k[t]/t^2)^\times$. Comme tout idéal propre est inclus dans $(k[t]/t^2) \setminus (k[t]/t^2)^\times = (t)$ (sinon l'idéal contient un inversible et n'est pas propre), on obtient par le théorème de correspondance que les idéaux propres de $k[t]/t^2$ sont en bijection avec les idéaux J de $k[t]$ tel que

$$(t^2) \subset J \subset (t).$$

Mais comme $(t)/(t^2)$ est un k-espace vectoriel de dimension 1, on voit que $J = (t^2)$ ou $J = (t)$.

On conclut que les idéaux sont : l'idéal impropre, l'idéal nul et l'unique idéal maximal (t).

(b) Let $I \subseteq M \subseteq A$ be two ideal in A. By Proposition 1.4.41 we have that:

$$A/M \cong (A/I)\big/\pi(M).$$

Now M is a maximal ideal in A if and only if A/M is a field. Now, by the above, A/M is a field if and only if $(A/I)\big/\pi(M)$ is a field, hence if and only if $\pi(M)$ is a maximal ideal in A/I.

Exercice 2. (a) Let $f(t), g(t) \in A[t]$. We have that

$$\mathrm{ev}(f+g)(a) = (f+g)(a) = f(a) + g(a) = \mathrm{ev}(f)(a) + \mathrm{ev}(g)(a) = (\mathrm{ev}(f) + \mathrm{ev}(g))(a)$$

for all $a \in A$. Therefore $\mathrm{ev}(f+g) = \mathrm{ev}(f) + \mathrm{ev}(g)$.

Similarly,

$$\mathrm{ev}(fg)(a) = (fg)(a) = f(a)g(a) = \mathrm{ev}(f)(a)\,\mathrm{ev}(g)(a) = (\mathrm{ev}(f)\,\mathrm{ev}(g))(a)$$

for all $a \in A$. Therefore $\mathrm{ev}(fg) = \mathrm{ev}(f)\,\mathrm{ev}(g)$.

Lastly, we have that $\mathrm{ev}(1)(a) = 1$ for all $a \in A$ and thus $\mathrm{ev}(1) = 1$, where the constant polynomial function 1 is the unity of $\mathcal{F}(A)$.

(b) Let $A = \mathbb{Z}/p\mathbb{Z}$ and let $f(t) = t^p - t \in A[t]$. Then $\mathrm{ev}(f)(a) = f(a) = a^p - a = 0$ for all $a \in A$ and thus $f \in \ker(\mathrm{ev})$.

(c) Let $A = \mathbb{R}$ and let $f(t) \in \ker(\mathrm{ev})$. Then, for all $a \in \mathbb{R}$ we have that $\mathrm{ev}(f)(a) = f(a) = 0$, which implies that all elements of $\mathbb{R}$ are roots of f. As f can have at most $\deg(f)$ real roots, we conclude that $f = 0$.

Exercice 3. 1. Soit $f(x,y) \in k[x,y]/(x^2y^3)$ nilpotent. On écrit $f(x,y) = xyh_1(x,y) + xh_2(x) + yh_2(y) + \lambda$, avec $\lambda \in k$. Comme xy est nilpotent, il suit que $xh_2(x) + yh_2(y) + \lambda$ est nilpotent. Comme l'image dans le quotient par (x) et (y) dans $k[y]$ et $k[x]$ respectivement est encore nilpotente et que ces anneaux sont intègres, il suit que $h_2(x) = h_2(y) = \lambda = 0$. Dès lors on conclut que $\mathrm{nil}(A) = (xy)$.

On peut aussi utiliser que les éléments nilpotents sont l'intersection de tous les premiers (Théorème 2.5.17). Comme (x) *et* (y) *sont premiers, on a* $\mathrm{nil}(A) \subset (x) \cap (y) = (xy)$. *Comme l'autre inclusion est également vérifiée, on a égalité.*

2. Notons que $(x) \cap (y) = (xy)$. En effet si $f(x,y) \in (x) \cap (y)$ alors $f(x,y) = xh_1(x,y) = yh_2(x,y)$. Comme (x) est un idéal premier, et que $y \notin (x)$ il suit que $h_2(x,y) \in (x)$, et donc que $f(x,y) \in (xy)$. Dès lors $\mathrm{nil}(A) = (x) \cap (y)$. Cette intersection est bien minimale, en effet sinon $\mathrm{nil}(A)$ serait premier. Mais $x, y \notin \mathrm{nil}(A)$ et $xy \in \mathrm{nil}(A)$.

3. Si $\mathfrak{p}$ est un premier qui contient x^2y^3, alors x ou y appartient à $\mathfrak{p}$ comme cet idéal est premier. Ainsi (x) ou (y) est inclus dans $\mathfrak{p}$. Comme ces idéaux sont premiers on conclut que ces premiers sont minimaux. En effet, en utilisant le raisonnement précédent si $\mathfrak{p} \subset (x)$, alors soit $(y) \subset \mathfrak{p} \subset (x)$ ou $(x)\mathfrak{p} \subset (x)$. Dans le deuxième cas, on a $\mathfrak{p} = (x)$. Notez que le premier cas est impossible car $y \notin (x)$. Ainsi (x) est minimal. Un raisonnement symétrique pour y s'applique.

   On avait d'abord pensé à cette preuve trop alambiquée.

   On avait donné en indication,

   Pour ce dernier point, on fait remarquer le fait suivant. Si A commutatif et $I_1, \ldots I_r$ des idéaux et $\mathfrak{p}$ un idéal premier, alors si $\cap_{i=1}^r I_i \subset \mathfrak{p}$, alors il existe j tel que $I_j \subset \mathfrak{p}$.

   Pour prouver cela, notons que si par l'absurde $i_k \in I_k \setminus \mathfrak{p}$ pour tout les k, alors $i_1 \cdots i_r \in \mathfrak{p}$. Mais comme $\mathfrak{p}$ est premier, on obtient une contradiction. En particulier si

$$\mathrm{nil}(A) = \mathfrak{p}_1 \cap \mathfrak{p}_2$$

   comme dans le cas de l'exercice, en utilisant que $\mathrm{nil}(A)$ contient tout les premiers, si $\mathfrak{p}$ est minimal, on a $\mathfrak{p}_1 \cap \mathfrak{p}_2 \subset \mathfrak{p}$ et donc en utilisant le lemme et la minimalité $\mathfrak{p}_i = \mathfrak{p}$ pour $i = 1$ ou $i = 2$. Ainsi on conclut dans le cas de l'exercice que l'ensemble des premiers minimaux (qui est non-vide, voir remarque après la preuve) est contenu dans $\{(x), (y)\}$. Or comme $\mathrm{nil}(A)$ n'est pas premier, il ne peut exister un unique premier minimal, et donc les idéaux premiers minimaux sont (x) et (y).

   Remarque. On note que tout idéal premier contient un premier minimal par le lemme de Zorn. (On vérifie qu'une intersection emboîtée de premiers est encore un idéal premier.)

Exercice 4. (a) We first note that $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ is an $\mathbb{F}_p$-algebra: $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ is a commutative ring and $\psi : \mathbb{F}_p \to \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ given by $\psi(a) = a \cdot [0]$, for $a \in \mathbb{F}_p$, is a ring homomorphism with the property that $\psi(\mathbb{F}_p) \subseteq \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$. In particular, we have that $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ is an $\mathbb{F}_p$ vector space with basis $\{[0], [g], [2g], \ldots, [(p-1)g]\}$, where $[g]$ is a fixed generator of $\mathbb{Z}/p\mathbb{Z}$.

We now consider the evaluation homomorphism

$$\mathrm{ev}_{[g]} : \mathbb{F}_p[x] \to \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$$
$$\mathrm{ev}_{[g]}(x) = 1 \cdot [g].$$

We have that $(x^p - 1) \subseteq \ker(\mathrm{ev}_{[g]})$, as $\mathrm{ev}_{[g]}(x^p - 1) = 1 \cdot [pg] - 1 \cdot [0] = 0$. On the other hand, as $\mathbb{F}_p$ is a field, by Corollary 2.2.5, it follows that $\mathbb{F}_p[x]$ is a principal ring and thus there exists $f \in \mathbb{F}_p[x]$ such that $\ker(\mathrm{ev}_{[g]}) = (f)$. Therefore, as $x^p - 1 \in (f)$, it follows that $x^p - 1 = f \cdot g$ for some $g \in \mathbb{F}_p[x]$ and by Lemma 2.1.1 we deduce that $\deg(f) \leq p$.

We write $f(x) = \sum_{i=0}^{p} a_i x^i$, where $a_i \in \mathbb{F}_p$. Then:

$$\mathrm{ev}_{[g]}(f(x)) = \sum_{i=0}^{m} a_i \cdot [ig] = (a_0 + a_p) \cdot [0] + \sum_{i=1}^{p-1} a_i \cdot [ig] = 0$$

and, as $[0], [g], [2g], \ldots, [(p-1)g]$ are linearly independent, we have $a_0 = -a_p$ and $a_i = 0$ for all $1 \leq i \leq p-1$. We deduce that $f(x) = a_p(x^p - 1)$, where $a_p \in \mathbb{F}_p$, and thus $\ker(\mathrm{ev}_{[g]}) = (x^p - 1)$. In conclusion, we have shown that $\mathbb{F}_p[x]/(x^p - 1) \cong \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$.

(b) Recall that the characteristic is the natural number n such that $n\mathbb{Z}$ is the kernel of the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$. Note the unique ring homomorphism from $\mathbb{Z}$ to $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ sends $x \in \mathbb{Z}$ to $[x]_p \in \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$. Its kernel is $p\mathbb{Z}$ therefore $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ has characteristic p.

(c) Let $a = \sum_{i=0}^{p-1} a_i' \cdot ([g]-1)^i$ be an idempotent element of $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$. Then

$$a^2 = \sum_{i,j} a_i a_j \cdot [(i+j)g] = \sum_{k=0}^{p-1} a_k \cdot [kg] = a$$

and, as $[0], [g], \ldots, [(p-1)g]$ are linearly independent, it follows that $a_k = \sum_{i+j=k} a_i a_j$ for all $0 \leq k \leq p-1$. In particular, we have $a_0 = a_0^2$ and so $a_0 = 0$ or $a_0 = 1$. As $a_1 = a_0 a_1 + a_1 a_0$ we see that in both cases we obtain $a_1 = 0$. Recursively, we deduce that

$$a_{k+1} = \sum_{i+j=k+1} a_i a_j = a_0 a_{k+1} + \Big(\sum_{\substack{i+j=k+1 \\ 1 \leq i,j \leq k}} a_i a_j \Big) + a_0 a_{k+1} = a_0 a_{k+1} + a_{k+1} a_0$$

and therefore $a_{k+1} = 0$. Hence, if $a_0 = 0$, it follows that $a = 0 \cdot [0]$, while, if $a_0 = 1$, it follows that $a = 1 \cdot [0]$. We have shown that the only idempotents of $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ are $0 \cdot [0]$ and $1 \cdot [0]$. By Proposition 2.4.55 and Remark 2.4.56 we conclude that $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ cannot be decomposed as a product of non-zero rings.

On propose également une résolution qui évite tout calcul.

On montre le petit lemme suivant qui peut être utile.

Lemme. Soit A un anneau commutatif tel que $A \setminus A^\times$ est un idéal. Alors c'est l'unique idéal maximal de A.

Preuve. Notons que tout idéal propre est contenu dans $A \setminus A^\times$. En effet si un élément inversible appartient à un idéal, celui-ci est forcément égal à A. Dès lors si $\mathfrak{m}$ est maximal (en particulier propre), on a $\mathfrak{m} \subset A \setminus A^\times$. Mais comme on a supposé que $A \setminus A^\times$ est un idéal, on a par maximalité $\mathfrak{m} = A \setminus A^\times$.

Maintenant, notons qu'un produit d'anneaux $A \times B$ non-nuls contient toujours au-moins deux idéaux maximaux : si $\mathfrak{m}_A$ et $\mathfrak{m}_B$ sont des idéaux maximaux de A et B respectivement, alors $\mathfrak{m}_A \times B$ et $A \times \mathfrak{m}_B$ sont maximaux.

Maintenant, dans l'anneau

$$A = \mathbb{F}_p[t]/(t-1)^p,$$

notons que $t-1$ est nilpotent. Si $f(t) \in \mathbb{F}_p[t]$, on peut écrire

$$f(t) = f(1) + (t-1)g(t)$$

par division euclidienne. Ainsi l'image dans le quotient $\overline{f(t)}$ peut s'écrire $\overline{f(t)} = f(1) - n$ avec $n \in A$ nilpotent. Dès lors, on voit que* $\overline{f(t)}$ est inversible si et seulement si $f(1) \neq 0$ ou autrement dit $\overline{f(t)} \notin (\bar{t}-1) = \ker(ev_1)$. Ainsi on a $A \setminus A^\times = (\bar{t}-1)$ qui est un idéal, et donc l'unique idéal maximal. Dès lors, il suit que A ne peut être un produit de deux anneaux non-nuls.

*si $\lambda \in A^\times$ et $n \in A$ nilpotent, alors $\lambda - n$ est inversible. En effet,

$$\frac{1}{\lambda - n} = \frac{1}{\lambda} \sum_{i=0}^{\infty} (n/\lambda)^i.$$

Exercice 5. 1. We define $\overline{a+b\sqrt{5}} = a - b\sqrt{5}$ and note that for all $z \in \mathbb{Z}[\sqrt{5}]$, the norm $N(z) = z\overline{z}$. The fact that N is a multiplicative function then follows from the fact that $\forall y, z \in \mathbb{Z}[\sqrt{5}]$, it holds that $\overline{yz} = \overline{y}\,\overline{z}$. With this, we get that $N(yz) = yz\overline{yz} = yz\overline{y}\,\overline{z} = y\overline{y}z\overline{z} = N(y)N(z)$.

Furthermore, if $z \in \mathbb{Z}[\sqrt{5}]$ is invertible, then $N(z) = \pm 1$ is necessary. If we denote its inverse by z^{-1}, then $N(z)N(z^{-1}) = N(1) = 1$, and therefore, $N(z) = \pm 1$. On the other hand, if $N(z) = \pm 1$ for some $z \in \mathbb{Z}[\sqrt{5}]$, then $\pm 1 = N(z) = z\overline{z}$ and hence $\pm\overline{z}$ is the inverse of z.

2. We note that $N(9+4\sqrt{5}) = 9^2 - 5 \cdot 4^2 = 1$, and so by the first point, $9+4\sqrt{5}$ is invertible. Furthermore, by the multiplicative property of the norm, the norm of $(9+4\sqrt{5})^n$ is 1 as well, for $n \in \mathbb{N}$. This means that we have created infinitely many invertible elements, and $(\mathbb{Z}[\sqrt{5}])^\times$ is infinite.

3. We first show that no elements of norm 2 exist. For this, we note that $N(a+\sqrt{5}b) = a^2 - 5b^2$, which is equal to a^2 modulo 5, a square. But all squares in $\mathbb{Z}/5\mathbb{Z}$ are either 0,1 or 4, as one checks by taking the square of all elements in $\mathbb{Z}/5\mathbb{Z}$.

   Now let $z \in \mathbb{Z}[\sqrt{5}]$ be of norm 4, and we assume that $z = v \cdot w$ for $v, w \in \mathbb{Z}[\sqrt{5}]$. Then $4 = N(z) = N(v)N(w)$. But as there are no elements of norm 2, we have that either $N(v) = \pm 1, N(w) = \pm 4$ or $N(v) = \pm 4, N(w) = \pm 1$. In either cases one of the two elements is of norm ± 1, which means that that element is invertible. Hence z is irreducible.

4. We have

   - $4 = 2 \cdot 2$ and $N(2) = 4$, hence by the previous part, 2 is irreducible
   - $4 = (1+\sqrt{5})(-1+\sqrt{5})$ and $N(1+\sqrt{5}) = -4, N(-1+\sqrt{5}) = -4$, hence both $1+\sqrt{5}, -1+\sqrt{5}$ are irreducible.
   - $4 = (3+\sqrt{5})(3-\sqrt{5})$ and $N(3+\sqrt{5}) = 4, N(3-\sqrt{5}) = 4$, hence both $3+\sqrt{5}, 3-\sqrt{5}$ are irreducible.

5. As we see from the previous point, $2 \cdot 2 = 4 = (3+\sqrt{5})(3-\sqrt{5})$, from which it follows that $2 \cdot 2 \in (3+\sqrt{5})$. But as $2 \notin (3+\sqrt{5})$, the ideal $(3+\sqrt{5})$ is not prime.

   We remark (all these notions will be defined later in the course) that irreducible does not imply prime in a ring that is not factorial or principal.

Exercice 6. 1. Soit $x = a + bi\sqrt{d} \in A$ avec $a^2 + b^2 d \leq d + 1$. Donc

$$a^2 + (b^2 - 1)d \leq 1.$$

On voit dès lors que $|b| \leq 1$. On distingue deux cas. Tout d'abord traitons le cas où $b = \pm 1$. Alors on a nécessairement $a = 0$ ou $a = \pm 1$, c'est à dire

$$x = \pm i\sqrt{d} \quad x = \pm(1 - i\sqrt{d}) \quad x = \pm(1 + i\sqrt{d}).$$

Traitons maintenant le cas où $b = 0$. On alors $x = a \in \mathbb{Z}$ avec la condition que $|a| \leq \sqrt{1+d}$.

2. On montre d'abord que $i\sqrt{d}$ est irréductible. On a $N(i\sqrt{d}) = d$. Ainsi si $x \mid i\sqrt{d}$ avec x ni inversible ni associé, il faut que $1 < N(x) < d$. Selon la liste établie au point 1, on a alors $x = a \in \mathbb{Z}$ avec $|a| < \sqrt{d}$. Mais comme on a supposé que $x \mid i\sqrt{d}$, il existe $e, f \in \mathbb{Z}$ tel que

$$a(e + fi\sqrt{d}) = i\sqrt{d}.$$

   Donc $e = 0$ et $fa = 1$ ce qui contredit $N(a) > 1$.

   On montre maintenant que $1 + i\sqrt{d}$ est irréductible. Comme la conjugaison complexe est un automorphisme d'anneau qui envoie $1 + i\sqrt{d}$ sur $1 - i\sqrt{d}$ cela montrera que $1 - i\sqrt{d}$ est également irréductible. Comme $N(1 + i\sqrt{d}) = 1 + d$, si $x \mid 1 + i\sqrt{d}$ avec x ni irréductible ni associé à $1 + i\sqrt{d}$, alors $1 < N(x) < 1 + d$. Comme il faut aussi que $N(x) \mid 1 + d$, on voit que $N(x) < d$. Ainsi un argument similaire à celui au-dessus conclut.

3. Supposons que $1+d$ n'est pas premier dans $\mathbb{Z}$. Alors on a
$$1+d=(1+i\sqrt{d})(1-i\sqrt{d})=p_1\cdots p_r$$
pour $p_1,\ldots,p_r$ des premiers avec $p_i\le d$ comme on a supposé $d+1$ pas premier. Comme $1+i\sqrt{d}$ est irréductible, si $1+d$ admet une factorisation *unique* en produit d'irréductibles (en supposant par l'absurde que A est factoriel) cela impliquerait que $1+i\sqrt{d}\mid p_j$ pour un indice j. Mais dès lors il existerait $e,f\in\mathbb{Z}$ avec
$$(1+i\sqrt{d})(e+fi\sqrt{d})=p_j$$
Donc $e+f=0$ et $p_j=e-df=(1+d)e$. Comme $p_j\le d$, c'est une contradiction. Ainsi on conclut que $1+d$ n'admet pas de factorisation unique en produit d'irréductibles. En particulier, on conclut que dans ce cas A n'est pas factoriel.

4. Supposons maintenant $q:=1+d$ premier dans $\mathbb{Z}$. On a
$$1+d=(1+i\sqrt{d})(1-i\sqrt{d}),$$
qui est une décomposition en irréductibles. On veut montrer que si $x\mid 1+d$ et est ni inversible ni associé à $1+d$, alors x est associé à $1+i\sqrt{d}$ ou $1-i\sqrt{d}$. Comme $N(1+d)=(1+d)^2=q^2$, un tel diviseur x satisfait forcément $N(x)=q=1+d$. Selon la liste au-dessus on a dès lors
$$x=\pm(1-i\sqrt{d})\quad x=\pm(1+i\sqrt{d}).$$
ou $x\in\mathbb{Z}$ avec $x^2=q$, mais cela n'est pas possible comme q est premier.

Exercice 7. (a) Let $\sum_{g\in G} a_g\cdot g\in\mathbb{Z}(A)$ and let $h\in G$. Then $1\cdot h\in A$ is invertible with inverse $(1\cdot h)^{-1}=1\cdot h^{-1}$ and we have
$$(1\cdot h)(\sum_{g\in G}a_g\cdot g)(1\cdot h)^{-1}=\sum_{g\in G}a_g\cdot hgh^{-1}=\sum_{g'\in G}a_{h^{-1}g'h}\cdot g'=\sum_{g'\in G}a_{g'}\cdot g'.$$
It follows that $a_{h^{-1}gh}=a_g$ for all $h\in G$ and thus the map $g\to a_g$ is constant over equivalence classes.

Conversely, assume that $g\to a_g$ is constant over equivalence classes. Let $1\cdot h\in A$. Then:
$$(1\cdot h)(\sum_{g\in G}a_g\cdot g)(1\cdot h)^{-1}=\sum_{g'\in G}a_{h^{-1}g'h}\cdot g'=\sum_{g'\in G}a_{g'}\cdot g'$$
and thus
$$(1\cdot h)(\sum_{g\in G}a_g\cdot g)=(\sum_{g\in G}a_g\cdot g)(1\cdot h),\ \text{for all } h\in G.$$
Therefore
$$(\sum_{h\in G}a_h\cdot h)(\sum_{g\in G}a_g\cdot g)=\sum_{h\in G}a_h\cdot h\sum_{g\in G}a_g\cdot g=\sum_{h\in G}a_h(\sum_{g\in G}a_g g)h=(\sum_{g\in G}a_g\cdot g)(\sum_{h\in G}a_h\cdot h)$$
and consequently $\sum_{g\in G}a_g\cdot g\in\mathbb{Z}(A)$.

(b) Fix $A=\mathbb{C}[S_3]$. By (a) we have that $e_1,e_2,e_3\in\mathbb{Z}(A)$. We will now show that they are idempotents. First,
$$\begin{aligned}e_1^2&=\frac{1}{36}(\sum_{g\in S_3}g)(\sum_{h\in S_3}h)\\&=\frac{1}{36}\Big[\sum_{g\in S_3}g+\sum_{g\in S_3}g(12)+\sum_{g\in S_3}g(13)+\sum_{g\in S_3}g(23)+\sum_{g\in S_3}g(123)+\sum_{g\in S_3}g(132)\Big]\\&=\frac{1}{6}\sum_{g\in S_3}g=e_1.\end{aligned}$$

In the above we have used the fact that for all $x \in S_3$, the map $S_3 \to S_3$ sending $a \to ax$ is bijective. Hence $\sum_{g \in S_3} gx = \sum_{g \in S_3} g$ for all $x \in S_3$. Secondly,

$$\begin{aligned}
e_2^2 &= \frac{1}{36}(\sum_{g \in S_3} \operatorname{sgn}(g)g)(\sum_{h \in S_3} \operatorname{sgn}(h)h) \\
&= \frac{1}{36}\Big[\sum_{g \in S_3} \operatorname{sgn}(g)g - \sum_{g \in S_3} \operatorname{sgn}(g)g(12) - \sum_{g \in S_3} \operatorname{sgn}(g)g(13) - \sum_{g \in S_3} \operatorname{sgn}(g)g(23) + \\
&\quad + \sum_{g \in S_3} \operatorname{sgn}(g)g(123) + \sum_{g \in S_3} \operatorname{sgn}(g)g(132)\Big] \\
&= \frac{1}{36}\Big[\sum_{g \in S_3} \operatorname{sgn}(g)g - \sum_{g \in S_3} \operatorname{sgn}(g(12))g - \sum_{g \in S_3} \operatorname{sgn}(g(13))g - \sum_{g \in S_3} \operatorname{sgn}(g(23))g + \\
&\quad + \sum_{g \in S_3} \operatorname{sgn}(g(132))g + \sum_{g \in S_3} \operatorname{sgn}(g(123))g\Big] \\
&= \frac{1}{6}\sum_{g \in S_3} \operatorname{sgn}(g)g = e_2.
\end{aligned}$$

In the above we have used the fact that $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$ for all $\sigma, \tau \in S_3$.

Lastly, we will show that f_1 and f_2 are idempotents and that $f_1 f_2 = f_2 f_1 = 0$. We have that:

$$\begin{aligned}
f_1^2 &= \frac{1}{9}\Big[\operatorname{Id} + \varepsilon(123) + \varepsilon^2(132) + \varepsilon(123) + \varepsilon^2(132) + \operatorname{Id} + \varepsilon^2(132) + \operatorname{Id} + \varepsilon(123)\Big] \\
&= \frac{1}{3}\Big[\operatorname{Id} + \varepsilon(123) + \varepsilon^2(132)\Big] = f_1.
\end{aligned}$$

Analogously one shows that $f_2^2 = f_2$. Keeping in mind that $\varepsilon^2 + \varepsilon = -1$, we have

$$\begin{aligned}
f_1 f_2 &= \frac{1}{9}\Big[\operatorname{Id} + \varepsilon(123) + \varepsilon^2(132) + \varepsilon^2(123) + (132) + \varepsilon \operatorname{Id} + \varepsilon(132) + \varepsilon^2 \operatorname{Id} + (123)\Big] \\
&= \frac{1}{9}(1 + \varepsilon + \varepsilon^2)\Big[\operatorname{Id} + (123) + (132)\Big] = 0.
\end{aligned}$$

Analogously one shows that $f_2 f_1 = 0$. Therefore $e_3^2 = (f_1 + f_2)^2 = f_1^2 + f_1 f_2 + f_2 f_1 + f_2^2 = f_1 + f_2 = e_3$.

We have shown that e_1, e_2, e_3 are central idempotents. We will now show that they are pairwise orthogonal. We have

$$e_1 e_2 = \frac{1}{36}\Big[\sum_{g \in G} g - \sum_{g \in G} g(12) - \sum_{g \in G} g(13) - \sum_{g \in G} g(23) + \sum_{g \in G} g(123) + \sum_{g \in G} g(132)\Big] = 0.$$

Analogously one shows that $e_2 e_1 = 0$. We note that $e_3 = \frac{1}{3}(2\operatorname{Id} - (123) - (132))$. Then

$$e_1 e_3 = \frac{1}{18}\Big[2\sum_{g \in G} g - \sum_{g \in G} g(123) - \sum_{g \in G} g(132)\Big] = 0$$

and

$$\begin{aligned}
e_2 e_3 &= \frac{1}{18}\Big[2\sum_{g \in G} \operatorname{sgn}(g)g - \sum_{g \in G} \operatorname{sgn}(g)g(123) - \sum_{g \in G} \operatorname{sgn}(g)g(132)\Big] \\
&= \frac{1}{18}\Big[2\sum_{g \in G} \operatorname{sgn}(g)g - \sum_{h \in G} \operatorname{sgn}(h(132))h - \sum_{h \in G} \operatorname{sgn}(h(123))h\Big] \\
&= 0.
\end{aligned}$$

Now $e_1 + e_2 = \frac{1}{3}[\mathrm{Id} + (123) + (132)]$ is a central idempotent in A, as $(e_1 + e_2)^2 = e_1^2 + e_1e_2 + e_2e_1 + e_2^2 = e_1 + e_2$. Furthermore, one checks that $(e_1 + e_2)e_3 = 0$ and $e_1 + e_2 + e_3 = \mathrm{Id}$. Thus, by Proposition 1.4.55, we have that $A \cong A(e_1 + e_2) \times Ae_3$.

Similarly, e_1 and e_2 are central orthogonal idempotents in $A(e_1 + e_2)$ and, as $e_1 + e_2$ is the identity in $A(e_1+e_2)$, we once more apply Proposition 1.4.55 to obtain $A(e_1+e_2) \cong Ae_1 \times Ae_2$. We have shown that:

$$A \cong Ae_1 \times Ae_2 \times Ae_3.$$

(c) Let $x \in Ae_1$. Then $x = ye_1$, where $y = a_0 \mathrm{Id} + a_1(12) + a_2(13) + a_3(23) + a_4(123) + a_5(132) \in A$. We compute

$$\begin{aligned} x &= a_0 \sum_{g\in G} g + a_1 \sum_{g\in G} g(12) + a_2 \sum_{g\in G} g(13) + a_3 \sum_{g\in G} g(23) + a_4 \sum_{g\in G} g(123) + a_5 \sum_{g\in G} g(132) \\ &= (a_0 + a_1 + a_2 + a_3 + a_4 + a_5) \sum_{g\in G} g \\ &= (\sum_{i=0}^{5} a_i)e_1. \end{aligned}$$

Therefore if $x \in Ae_1$ then $x = c_xe_1$, for some $c_x \in \mathbb{C}$. Analogously, one shows that if $x \in Ae_2$ then $x = c_xe_2$, for some $c_x \in \mathbb{C}$. (In this case, computations will show that $c_x = a_0 - a_1 - a_2 - a_3 + a_4 + a_5$.)

For $i = 1, 2$ consider the map $\varphi : Ae_i \to \mathbb{C}$ given by $\varphi(x) = c_x$. One checks that φ is a ring isomorphism and concludes that $Ae_i \cong \mathbb{C}$, for $i = 1, 2$.

(d) Let $x \in Ae_3$. Then $x = ye_3$, where $y = a_0 \mathrm{Id} + a_1(12) + a_2(13) + a_3(23) + a_4(123) + a_5(132) \in A$. We compute

$$yf_1 = (a_0 + a_5\varepsilon + a_4\varepsilon^2)f_1 + (a_1 + a_2\varepsilon + a_3\varepsilon^2)(12)f_1$$

and

$$yf_2 = (a_0 + a_4\varepsilon + a_5\varepsilon^2)f_2 + (a_1 + a_3\varepsilon + a_2\varepsilon^2)(12)f_2$$

to determine that

$$\begin{aligned} x &= (a_0 + a_5\varepsilon + a_4\varepsilon^2)f_1 + (a_1 + a_2\varepsilon + a_3\varepsilon^2)(12)f_1 + (a_0 + a_4\varepsilon + a_5\varepsilon^2)f_2 + (a_1 + a_3\varepsilon + a_2\varepsilon^2)(12)f_2 \\ &= x_1f_1 + x_2(12)f_1 + x_3(12)f_2 + x_4f_2, \end{aligned}$$

where $x_1, x_2, x_3, x_4 \in \mathbb{C}$.

Define the map $\varphi : Ae_3 \to M_2(\mathbb{C})$ by $\varphi(x) = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix}$. Clearly φ is a bijective map, $\varphi(x + y) = \varphi(x) + \varphi(y)$ for all $x, y \in Ae_3$ and $\varphi(e_3) = \mathrm{I}_2$. What remains to show is that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in Ae_3$.

We first remark that

$$(12)f_1 = \frac{1}{3}[(12) + \varepsilon(23) + \varepsilon^2(13)] = f_2(12)$$

and

$$f_1(12) = \frac{1}{3}[(12) + \varepsilon(13) + \varepsilon^2(23)] = (12)f_2.$$

Now, keeping in mind that $f_1^2 = f_1$, $f_2^2 = f_2$, $f_1f_2 = f_2f_1 = 0$, $(12)f_1 = f_2(12)$ and

$f_1(12) = (12)f_2$, we have

$$\begin{aligned}
xy &= (x_1f_1 + x_2(12)f_1 + x_3(12)f_2 + x_4f_2)(y_1f_1 + y_2(12)f_1 + y_3(12)f_2 + y_4f_2) \\
&= x_1y_1f_1^2 + x_2y_1(12)f_1f_1 + x_3y_1(12)f_2f_1 + x_4y_1f_2f_1 + x_1y_2f_1(12)f_1 + x_2y_2(12)f_1(12)f_1 + \\
&+ x_3y_2(12)f_2(12)f_1 + x_4y_2f_2(12)f_1 + x_1y_3f_1(12)f_2 + x_2y_3(12)f_1(12)f_2 + x_3y_3(12)f_2(12)f_2 + \\
&+ x_4y_3f_2(12)f_2 + x_1y_4f_1f_2 + x_2y_4(12)f_1f_2 + x_3y_4(12)f_2f_2 + x_4y_4f_2^2 \\
&= x_1y_1f_1 + x_2y_1(12)f_1 + x_3y_2f_1 + x_4y_2(12)f_1 + x_1y_3(12)f_2 + x_2y_3f_2 + x_3y_4(12)f_2 + x_4y_4f_2 \\
&= (x_1y_1 + x_3y_2)f_1 + (x_2y_1 + x_4y_2)(12)f_1 + (x_1y_3 + x_3y_4)(12)f_2 + (x_2y_3 + x_4y_4)f_2.
\end{aligned}$$

Thus $\varphi(xy) = \begin{pmatrix} x_1y_1 + x_3y_2 & x_1y_3 + x_3y_4 \\ x_2y_1 + x_4y_2 & x_2y_3 + x_4y_4 \end{pmatrix} = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix} \cdot \begin{pmatrix} y_1 & y_3 \\ y_2 & y_4 \end{pmatrix} = \varphi(x)\varphi(y)$. We conclude that φ is a ring isomorphism and thus $Ae_3 \cong M_2(\mathbb{C})$.