Elements of solution for Homework 6

Chapter 17

F.1

If $(G, +)$ is an abelian group, then $\mathrm{End}(G)$, equipped with pointwise addition is a subgroup of the additive group of functions from G to itself. The neutral element is the constant map $g \mapsto 0_G$ and the inverse of $u \in \mathrm{End}(G)$ is the map $-u : g \mapsto -u(x)$.

As for the multiplicative structure, composition is associative on functions from G to itself and a composition of homomorphisms is a homomorphism so $\circ$ is an internal composition law on $\mathrm{End}(G)$ for which the identical map $g \mapsto g$ is an identity.

To check distributivity, let u, v and w be elements in $\mathrm{End}(G)$. Then, for any $g \in G$,

$$\begin{array}{rcll} u \circ (v+w)(g) & = & u\left((v+w)(x)\right) & \\ & = & u(v(x)+w(x)) & \text{by definition of the addition on } \mathrm{End}(G) \\ & = & u(v(x))+u(w(x)) & \text{because } u \text{ is a morphism} \\ & = & u \circ v(x) + u \circ w(x) & \end{array}$$

so $u \circ (v+w) = u \circ v + u \circ w$.

Similarly,

$$\begin{array}{rcll} \left((v+w) \circ u\right)(g) & = & (v+w)\left(u(x)\right) & \\ & = & v(u(x))+w(u(x)) & \text{by definition of the addition on } \mathrm{End}(G) \\ & = & v \circ u(x) + w \circ u(x) & \end{array}$$

so[1] $(v+w) \circ u = v \circ u + w \circ u$.

[1] Notice that the fact that the maps are homomorphisms is not necessary to prove distributivity on that side.

F.2

To determine all the endomorphisms of $\mathbb{Z}/4\mathbb{Z}$, we notice that any homomorphism from a cyclic group to another group (cyclic or not) is determined by the image of a generator.

More precisely, if $(G,+) = \langle a \rangle$, then any element $g \in G$ is of the form $a + a + \ldots + a$ or $(-a) + (-a) + \ldots + (-a)$, that is

$$g = n \cdot a$$

for some $n \in \mathbb{Z}$. Now, if G' is any group (denoted multiplicatively) and $\varphi \in \mathrm{Hom}(G, G')$, we get

$$\varphi(g) = \varphi(n \cdot a) = \varphi(a)^n$$

so the knowledge of $\varphi(a)$ characterizes φ.

In the particular case of $G = \mathbb{Z}/4\mathbb{Z} = \langle 1 \rangle$ and $G' = \mathbb{Z}/4\mathbb{Z}$ with additive notation, the previous relation become

$$(\dagger) \qquad \varphi(n) = n\varphi(1).$$

For $k \in \{0,1,2,3\}$, we will denote by φ_k the map

$$\begin{array}{ccc} \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \\ n & \longmapsto & kn \end{array}.$$

Then $\mathrm{End}(\mathbb{Z}/4\mathbb{Z}) = \{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}$ and we will prove that the map

$$\begin{array}{ccc} \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathrm{End}(\mathbb{Z}/4\mathbb{Z}) \\ k & \longmapsto & \varphi_k \end{array}$$

is an isomorphism of rings[2]. Straightforward calculations show that

$$\varphi_{k+k'} = \varphi_k + \varphi_{k'} \qquad \text{and} \qquad \varphi_{kk'} = \varphi_k \circ \varphi_{k'}.$$

To prove bijectivity, one can either prove injectivity and notice that surjectivity follows from $(\dagger)$ or verify that the map

$$\begin{array}{ccc} \mathrm{End}(\mathbb{Z}/4\mathbb{Z}) & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \\ \varphi & \longmapsto & \varphi(1) \end{array}$$

is an inverse for the map under study. Therefore, $\mathrm{End}(\mathbb{Z}/4\mathbb{Z})$ has the same tables as $\mathbb{Z}/4\mathbb{Z}$.

[2]This generalizes to $\mathrm{End}(\mathbb{Z}/n\mathbb{Z})$ for any n.

Chapter 18

A.1

Use the subgring criterion.

A.6

Same method. Notice that the map $\left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathrm{M}_2(\mathbb{R}) \\ x & \longmapsto & \left[\begin{array}{cc} 0 & 0 \\ 0 & x \end{array} \right] \end{array} \right.$ is an ring isomorphism.

B.1

The diagonal subring $\{(n,n)\ ,\ n \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$ but it is not absorbent.

The map $\left\{ \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z} \\ (a,b) & \longmapsto & ([a],b) \end{array} \right.$ is a ring homomorphism so its kernel $5\mathbb{Z} \times \{0\}$ is an ideal.

The subset $\{(m,n)\ ,\ m+n \in 2\mathbb{Z}\}$ is a subring of $\mathbb{Z} \times \mathbb{Z}$ but it is not absorbent.

The subset $\{(m,n)\ ,\ mn \in 2\mathbb{Z}\}$ of $\mathbb{Z} \times \mathbb{Z}$ is not stable under addition.

The map $\left\{ \begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ (a,b) & \longmapsto & ([a],[b]) \end{array} \right.$ is a ring homomorphism so its kernel $2\mathbb{Z} \times 3\mathbb{Z}$ is an ideal.

B.5

The product of a continuous function (such as $x \mapsto 1$) with a discontinuous function need not be continuous so $\mathcal{C}(\mathbb{R})$ is not an ideal in $\mathcal{F}(\mathbb{R})$.

H.5

Follow the hints of the textbook, keeping in mind that a function is invertible if and only if it never vanishes. It is ok to use the result of Exercise **D.5**, which we established in class.

I.1

The more general result is that if f is a ring homomorphism from A to B and I is an ideal in A, then $f(I)$ is an ideal in $f(A)$[3].

We have proved earlier that the homomorphic image of a subgroup is a subgroup so $(f(I), +)$ is a subgroup of $(f(A), +)$.

To prove that it is an ideal, we show that for any $b \in f(A)$ and $y \in f(I)$, the products by and yb are elements of $f(I)$. To do so, let $a \in A$ and $x \in I$ be such that $f(a) = b$ and $f(x) = y$. Then

$$by = f(a)f(x) = f(ax) \qquad \text{and} \qquad yb = f(x)f(a) = f(xa)$$

because f is a ring homomorphism and $ax, xa \in I$ because I is an ideal so $f(I)$ is an ideal in $f(A)$.

Remarks:

- Note that the condition on the kernel given by the book was not used in the proof. To convince yourself that it is not necessary, consider $A = \mathbb{Z}$, $B = \mathbb{Z}/3\mathbb{Z}$, f the natural surjection: $f(n) = n \mod 3$ and $I = 2\mathbb{Z}$.
- In general, $f(I)$ is **not** an ideal in A. Consider for instance the image of $\mathbb{R}$ under the inclusion map $\mathbb{R} \longrightarrow \mathbb{R}[X]$.

I.2

Assume that f is a surjective morphism f between a ring A and a field B. To prove that $\ker f$ is a maximal ideal in A, we shall prove that any ideal I that strictly contains $\ker f$ must contain an invertible element and is therefore equal to A by a result proven in class.

By the result of the previous question, $f(I)$ is an ideal in B. Since fields have no non-trivial ideals, $f(I)$ must be $\{0\}$ or A. Since I contains elements that are not in $\ker f$, we know that $f(I) \neq \{0\}$ so $f(I) = B$.

Let x be an element of I such that $x \notin \ker f$. Then $f(x) \neq 0$ so $f(x)$ is invertible in the field B. Since $f(I) = B$, the inverse of $f(x)$ belongs to $f(I)$. In other words,

$$\exists x_0 \in I \ , \ f(x_0) = f(x)^{-1}.$$

Note that even though f is a ring homomorphism, **there is no reason to assume that x is invertible** and that $f(x)^{-1} = f(x^{-1})$...

[3]The surjectivity assumption guarantees $f(A) = B$.

However, the equation $f(x_0)f(x) = 1_B = f(1_A)$ implies that

$$f(x_0x - 1_A) = 0.$$

In other words, $x_0x - 1_A \in \ker f \subset I$. Therefore,

$$1_A = \underbrace{x_0x}_{\in I} - \underbrace{(x_0x - 1_A)}_{\in I}$$

so $1_A \in I$, which concludes the proof.

N.B. The proof can be made to work in the case where A does not contain an identity (done in the x-hour).

I.3

Arguing like in **F.2** (Chapter 17), we see that all group endomorphisms of $\mathbb{Z}$ are of the form $\varphi_k : n \mapsto kn$. For such a map to be a ring homomorphism, it is necessary that

$$k = \varphi_k(1) = \varphi_k(1 \cdot 1) = \varphi_k(1)\varphi_k(1) = k^2,$$

which implies that $k \in \{0, 1\}$. Conversely, one checks that the zero map φ_0 and the identity map φ_1 are ring endomorphisms of $\mathbb{Z}$.

Chapter 19

E.5

Let A be a ring and J and ideal such that every element in A/J is nilpotent. This means that for every X in A/J, there exists an integer $n \geq 0$ such that $X^n = 0_{A/J}$. Therefore, if x is an element of A, there exists an integer n such that

$$[x]^n = [x^n] = 0_{A/J}.$$

The representatives of $0_{A/J}$ are exactly the elements of J, so this implies that $x^n \in J$.

The converse holds, by the same type of argument.

F.1

The fact that the quotient of a ring A by an ideal J is a ring has been verified in class. If A is commutative, the relation $[a] \cdot [b] = [a \cdot b]$, which defines the product on A/J, implies that A/J is commutative too. The same relation also implies that if A has an identity 1_A, then $[1_A]$ is an identity for A/J.

F.2

Recall that an ideal J in a ring A is said *prime* if, for a and b in J

$$ab \in J \quad \Rightarrow \quad a \in J \text{ or } b \in J.$$

Let J be an ideal in a commutative ring A. Since an element $a \in A$ belongs to J if and only if $[a] = 0_{A/J}$, if X and Y are elements of A/J, the condition

$$XY = 0_{A/J}$$

is equivalent to the fact that

$$xy \in J$$

for any x, y representatives of X and Y in A. It follows that A/J has zero divisors if and only if J is not prime.

F.3

If J is a maximal ideal of a commutative ring A, then A/J is a field. In particular, A/J is an integral domain, which by the result proved in the previous questions, implies that J is prime.

F.4

To prove that if A/J is field, then J is maximal, it suffices to apply the result proved in **I.2** above to the case of the natural surjection

$$\begin{array}{rccc} \varpi : A & \longrightarrow & A/J \\ a & \longmapsto & [a] \end{array},$$

whose kernel is precisely J.