1 Exercise 1: The opposite ring

Let $\mathbb{K}$ be a ring. We define a new binary operation $\tilde{\cdot}$ on $\mathbb{K}$ by setting

$$a \tilde{\cdot} b = ba \quad \text{for all } a, b \in \mathbb{K}.$$ 

(Thus, $\tilde{\cdot}$ is the multiplication of $\mathbb{K}$, but with the arguments switched.)

(a) Prove that the set $\mathbb{K}$, equipped with the addition $+$, the multiplication $\tilde{\cdot}$, the zero $0_{\mathbb{K}}$ and the unity $1_{\mathbb{K}}$, is a ring.

This new ring is called the opposite ring of $\mathbb{K}$, and is denoted by $\mathbb{K}^{op}$.

Note that the sets $\mathbb{K}$ and $\mathbb{K}^{op}$ are identical (so a map from $\mathbb{K}$ to $\mathbb{K}$ is the same as a map from $\mathbb{K}$ to $\mathbb{K}^{op}$); but the rings $\mathbb{K}$ and $\mathbb{K}^{op}$ are generally not the same (so a ring homomorphism from $\mathbb{K}$ to $\mathbb{K}$ is not the same as a ring homomorphism from $\mathbb{K}$ to $\mathbb{K}^{op}$).

(b) Prove that the identity map $id : \mathbb{K} \to \mathbb{K}$ is a ring isomorphism from $\mathbb{K}$ to $\mathbb{K}^{op}$ if and only if $\mathbb{K}$ is commutative.

(c) Now, assume that $\mathbb{K}$ is the matrix ring $\mathbb{L}^{n \times n}$ for some commutative ring $\mathbb{L}$ and some $n \in \mathbb{N}$. Prove that the map

$$\mathbb{K} \to \mathbb{K}^{op}, \quad A \mapsto A^T$$

(where $A^T$, as usual, denotes the transpose of a matrix $A$) is a ring isomorphism.
[Hint: In (a), you only have to check the ring axioms that have to do with multiplication. Similarly, in (b), you are free to check the one axiom relating to multiplication only. In (c), you can use [Grinbe19 Exercise 6.5] without proof.]

1.1 Remark

This exercise gives some examples of rings $K$ that are isomorphic to their opposite rings $K^{op}$. See https://mathoverflow.net/questions/64370/ for examples of rings that are not.

1.2 Solution

We shall follow the PEMDAS convention for the order of operations, treating the new multiplication $\sim$ operation as a multiplicative operation. Thus, the expression \[ a \sim b + c \sim d \] will mean \[ (a \sim b) + (c \sim d) \] rather than \[ a \sim (b + c) \sim d. \]

We are in the slightly confusing situation of having two different “multiplications” on one and the same set $K$: the original multiplication of the ring $K$, and the new multiplication $\sim$ of the ring $K^{op}$ (although we still have not shown that $K^{op}$ is actually a ring). Let us agree that if $a, b \in K$, then the notation \[ ab \] shall always mean \[ a \cdot b \] (that is, the image of the pair $(a, b)$ under the original multiplication $\cdot$, not under the new multiplication $\sim$).

The original ring $K$ satisfies all eight ring axioms (since it is a ring).

(a) Clearly, the addition $+$ and the multiplication $\sim$ are binary operations on $K$, and the elements $0_K$ and $1_K$ indeed belong to $K$. It remains to prove that these two operations and these two elements make $K$ into a ring. In order to do so, we need to verify the ring axioms. These axioms are the following:

- **Commutativity of addition:** We have $a + b = b + a$ for all $a, b \in K$.
- **Associativity of addition:** We have $a + (b + c) = (a + b) + c$ for all $a, b, c \in K$.
- **Neutrality of zero:** We have $a + 0_K = 0_K + a = a$ for all $a \in K$.
- **Existence of additive inverses:** For any $a \in K$, there exists an element $a' \in K$ such that $a + a' = a' + a = 0_K$.
- **Associativity of multiplication:** We have $a \sim (b \sim c) = (a \sim b) \sim c$ for all $a, b, c \in K$. (Of course, we cannot use “$ab$” as an abbreviation for “$a \sim b$”, since “$ab$” already stands for the different product $a \cdot b$.)
- **Neutrality of one:** We have $a \sim 1_K = 1_K \sim a = a$ for all $a \in K$.
- **Annihilation:** We have $a \sim 0_K = 0_K \sim a = 0_K$ for all $a \in K$.
- **Distributivity:** We have $a \sim (b + c) = a \sim b + a \sim c$ and $(a + b) \sim c = a \sim c + b \sim c$ for all $a, b, c \in K$.

The first four of these eight axioms do not involve the new multiplication $\sim$. Thus, they say exactly the same thing as the corresponding axioms for the original ring $K$ (with the original operations $+$ and $\cdot$). Hence, they are satisfied (since the corresponding axioms for
the original ring $\mathbb{K}$ are satisfied. It thus remains to prove that the remaining four axioms are satisfied. Let us check this:

*Proof of the “Associativity of multiplication” axiom:* Let $a, b, c \in \mathbb{K}$. We must prove that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

The definition of the operation $\cdot$ yields $b \cdot c = cb$ and $a \cdot b = ba$ and

$$a \cdot (b \cdot c) = (b \cdot c) a = (cb) a$$

and

$$(a \cdot b) \cdot c = c (a \cdot b) = c (ba) .$$

But the original ring $\mathbb{K}$ satisfies the “Associativity of multiplication” axiom (since it is a ring); thus, $(cb) a = c (ba)$. In other words, the right hand sides of the two equalities (1) and (2) are equal. Thus, their left hand sides are also equal. In other words, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Thus, the “Associativity of multiplication” axiom is proven.

*Proof of the “Annihilation” axiom:* Let $a \in \mathbb{K}$. We must prove that $a \cdot 1_{\mathbb{K}} = 1_{\mathbb{K}} \cdot a = a$.

But the original ring $\mathbb{K}$ satisfies the “Annihilation” axiom (since it is a ring); thus, $a 1_{\mathbb{K}} = 1_{\mathbb{K}} a = a$.

The definition of the operation $\cdot$ yields $a \cdot 1_{\mathbb{K}} = 1_{\mathbb{K}} a = a$ and $1_{\mathbb{K}} \cdot a = a 1_{\mathbb{K}} = a$.

Combining these two equalities, we find $a \cdot 1_{\mathbb{K}} = 1_{\mathbb{K}} \cdot a = a$. Thus, the “Annihilation” axiom is proven.

*Proof of the “Neutrality of one” axiom:* Let $a \in \mathbb{K}$. We must prove that $a \cdot 0_{\mathbb{K}} = 0_{\mathbb{K}} \cdot a = 0_{\mathbb{K}}$.

But the original ring $\mathbb{K}$ satisfies the “Annihilation” axiom (since it is a ring); thus, $a 0_{\mathbb{K}} = 0_{\mathbb{K}} a = 0_{\mathbb{K}}$.

The definition of the operation $\cdot$ yields $a \cdot 0_{\mathbb{K}} = 0_{\mathbb{K}} a = 0_{\mathbb{K}}$ and $0_{\mathbb{K}} \cdot a = a 0_{\mathbb{K}} = 0_{\mathbb{K}}$.

Combining these two equalities, we find $a \cdot 0_{\mathbb{K}} = 0_{\mathbb{K}} \cdot a = 0_{\mathbb{K}}$. Thus, the “Annihilation” axiom is proven.

*Proof of the “Distributivity” axiom:* Let $a, b, c \in \mathbb{K}$. We must prove that

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and

$$(a + b) \cdot c = a \cdot c + b \cdot c .$$

But the original ring $\mathbb{K}$ satisfies the “Distributivity” axiom (since it is a ring); thus,

$$c (a + b) = ca + cb$$

and

$$(b + c) a = ba + ca .$$

The definition of the operation $\cdot$ yields $a \cdot (b + c) = (b + c) a$ and $a \cdot b = ba$ and $a \cdot c = ca$. Thus,

$$a \cdot (b + c) = (b + c) a = ba + ca .$$

Comparing this with $a \cdot b + a \cdot c = ba + ca$, we obtain $a \cdot (b + c) = a \cdot b + a \cdot c$.

The definition of the operation $\cdot$ yields $(a + b) \cdot c = c (a + b)$ and $a \cdot c = ca$ and $b \cdot c = cb$. Thus,

$$(a + b) \cdot c = c (a + b) = ca + cb .$$

Comparing this with $a \cdot c + b \cdot c = ca + cb$, we obtain $(a + b) \cdot c = a \cdot c + b \cdot c$.

Thus, we have proven the equalities

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and

$$(a + b) \cdot c = a \cdot c + b \cdot c .$$
Hence, the “Associativity of multiplication” axiom is proven.

We have now shown that the set \(K\), equipped with the addition \(+\), the multiplication \(\cdot\), the zero \(0_{K}\) and the unity \(1_{K}\), satisfies all eight ring axioms. Hence, it is a ring. This solves part (a) of the problem.

(b) \(\implies\): Assume that \(\text{id} : K \to K\) is a ring isomorphism from \(K\) to \(K^{\text{op}}\). We must prove that \(K\) is commutative.

We have assumed that \(\text{id}\) is a ring isomorphism from \(K\) to \(K^{\text{op}}\). Thus, in particular, \(\text{id}\) is a ring homomorphism from \(K\) to \(K^{\text{op}}\) (since any ring isomorphism must be a ring homomorphism).

Recall that if \(U\) and \(V\) are two rings, and if \(f\) is a ring homomorphism from \(U\) to \(V\), then
\[
 f(a \cdot b) = f(a) \cdot f(b) \quad \text{for all } a, b \in U. \tag{3}
\]
(Indeed, this is one of the four axioms in our definition of a ring homomorphism.) But keep in mind that the two “\(\cdot\)” signs in the equality \(\text{(3)}\) have different meanings: The “\(\cdot\)” sign on the left hand side stands for the multiplication of the ring \(U\), whereas the “\(\cdot\)” sign on the right hand side stands for the multiplication of the ring \(V\). Thus, \(\text{(3)}\) (applied to \(U = K\), \(V = K^{\text{op}}\) and \(f = \text{id}\)) yields
\[
 \text{id}(a \cdot b) = \text{id}(a) \cdot \text{id}(b) \quad \text{for all } a, b \in K \tag{4}
\]
(since \(\text{id}\) is a ring homomorphism from \(K\) to \(K^{\text{op}}\), and since the multiplication of the ring \(K\) is denoted by “\(\cdot\)” whereas the multiplication of the ring \(K^{\text{op}}\) is denoted by “\(\cdot^\sim\)”).

Now, if \(a, b \in K\), then
\[
 ab = a \cdot b = \text{id}(a \cdot b) = \text{id}(a) \cdot^\sim \text{id}(b) \quad \text{(by \(\text{(4)}\))}
 = a \cdot^\sim b = ba \quad \text{(by the definition of the operation } \cdot^\sim).\]
In other words, the ring \(K\) satisfies the “Commutativity of multiplication” axiom. In other words, the ring \(K\) is commutative. This proves the “\(\implies\)” direction of part (b).

\(\iff\): Assume that \(K\) is commutative. We must prove that \(\text{id} : K \to K\) is a ring isomorphism from \(K\) to \(K^{\text{op}}\).

If \(a, b \in K\), then
\[
 a \cdot^\sim b = ba \quad \text{(by the definition of the operation } \cdot^\sim)\]
\[
 = ab \quad \text{(since the ring } K\text{ is commutative)}
 = a \cdot b.
\]
Thus, the binary operation \(\cdot^\sim\) is identical with the binary operation \(\cdot\).

But the only difference between the rings \(K\) and \(K^{\text{op}}\) is that \(K^{\text{op}}\) has the multiplication \(\cdot^\sim\) while \(K\) has the multiplication \(\cdot\). (All the remaining structure of \(K\) and \(K^{\text{op}}\) is the same.) But since we have shown that \(\cdot^\sim\) is identical with \(\cdot\), we see that this difference is not actually a difference either; the multiplications of \(K\) and \(K^{\text{op}}\) are also the same. Hence, the ring \(K^{\text{op}}\) is completely identical to the ring \(K\) (not just as sets, but as rings with all their structure).

But recall that \(\text{id} : K \to K\) is a ring isomorphism from \(K\) to \(K\). Since the ring \(K^{\text{op}}\) is completely identical to the ring \(K\), we can replace the last “\(K\)” in this sentence by “\(K^{\text{op}}\)” without changing its meaning. Thus, we obtain that \(\text{id} : K \to K\) is a ring isomorphism from \(K\) to \(K^{\text{op}}\). This proves the “\(\iff\)” direction of part (b).

(c) Let us quote the following fact from [Grinbe19 Exercise 6.5] (except that we are replacing \(K\) by \(L\)):
Proposition 1.1. Let \( \mathbb{L} \) be a commutative ring. In this proposition, all matrices are over \( \mathbb{L} \).

(a) If \( u, v \) and \( w \) are three nonnegative integers, if \( P \) is a \( u \times v \)-matrix, and if \( Q \) is a \( v \times w \)-matrix, then

\[
(PQ)^T = Q^TP^T.
\]

(b) Every \( u \in \mathbb{N} \) satisfies

\[
(I_u)^T = I_u.
\]

(c) If \( u \) and \( v \) are two nonnegative integers, if \( P \) is a \( u \times v \)-matrix, and if \( \lambda \in \mathbb{L} \), then

\[
(\lambda P)^T = \lambda P^T.
\]

(d) If \( u \) and \( v \) are two nonnegative integers, and if \( P \) and \( Q \) are two \( u \times v \)-matrices, then

\[
(P + Q)^T = P^T + Q^T.
\]

(e) If \( u \) and \( v \) are two nonnegative integers, and if \( P \) is a \( u \times v \)-matrix, then

\[
(P^T)^T = P.
\]

Now, let \( T \) be the map

\[
\mathbb{K} \to \mathbb{K}^{\text{op}}, \quad A \mapsto A^T.
\]
We must prove that \( T \) is a ring isomorphism.

In class\(^1\) we have proven that any invertible ring homomorphism is a ring isomorphism. Hence, it suffices to prove that \( T \) is an invertible ring homomorphism.

Let us first prove that \( T \) is a ring homomorphism. In order to do so, we need to verify the following four claims:

**Claim 1:** We have \( T(a + b) = T(a) + T(b) \) for all \( a, b \in \mathbb{K} \).

**Claim 2:** We have \( T(0_\mathbb{K}) = 0_{\mathbb{K}^{\text{op}}} \).

**Claim 3:** We have \( T(ab) = T(a) \cdot T(b) \) for all \( a, b \in \mathbb{K} \).

**Claim 4:** We have \( T(1_\mathbb{K}) = 1_{\mathbb{K}^{\text{op}}} \).

(Note the “\( \cdot \)” sign on the right hand side of Claim 3; this is because \( T(a) \) and \( T(b) \) are being considered as elements of \( \mathbb{K}^{\text{op}} \), and the multiplication of the ring \( \mathbb{K}^{\text{op}} \) is \( \cdot \).)

Let us now prove these claims:

**Proof of Claim 3:** Let \( a, b \in \mathbb{K} \). Then, \( a \in \mathbb{L}^{n \times n} \) and \( b \in \mathbb{L}^{n \times n} \). Hence, \( a \) and \( b \) are two \( n \times n \)-matrices over \( \mathbb{L} \). The definition of \( T \) yields \( T(ab) = (ab)^T \) and \( T(a) = a^T \) and \( T(b) = b^T \). The definition of the operation \( \cdot \) yields \( T(a) \cdot T(b) = T(b) \cdot T(a) = b^T a^T \).

But \( T(ab) = (ab)^T = b^T a^T \) (by Proposition 1.1 (a), applied to \( u = n, v = n, w = n, P = a \) and \( Q = b \)). Comparing these two equalities, we obtain \( T(ab) = T(a) \cdot T(b) \). This proves Claim 3.

**Proof of Claim 1:** Let \( a, b \in \mathbb{K} \). Then, \( a \in \mathbb{L}^{n \times n} \) and \( b \in \mathbb{L}^{n \times n} \). Hence, \( a \) and \( b \) are two \( n \times n \)-matrices over \( \mathbb{L} \). The definition of \( T \) yields \( T(a + b) = (a + b)^T \) and \( T(a) = a^T \) and \( T(b) = b^T \). But \( T(a) + T(b) = a^T + b^T \). But \( T(a + b) = (a + b)^T = a^T + b^T \)

---

\(^1\)specifically, Proposition 5.10.5 in [the class notes](#); but the numbering may change
(by Proposition 1.1 (d), applied to $u = n$, $v = n$, $P = a$ and $Q = b$). Comparing these two equalities, we obtain $T(a + b) = T(a) + T(b)$. This proves Claim 1.

[Proof of Claim 2: We have $0_K = 0_{n \times n}$ (by the definition of the ring $K = \mathbb{L}^{n \times n}$). Applying the map $T$ to both sides of this equality, we obtain $T(0_K) = T(0_{n \times n}) = (0_{n \times n})^T$ (by the definition of $T$). But the definition of the transpose of a matrix easily yields $(0_{n \times n})^T = 0_{n \times n}$. Hence, $T(0_K) = (0_{n \times n})^T = 0_{n \times n}$. But the definition of the ring $K^{op}$ yields $0_{K^{op}} = 0_K = 0_{n \times n}$. Comparing the latter two equalities, we obtain $T(0_K) = 0_{K^{op}}$. This proves Claim 2.]

[Proof of Claim 4: We have $1_K = I_n$ (by the definition of the ring $K = \mathbb{L}^{n \times n}$). Applying the map $T$ to both sides of this equality, we obtain $T(1_K) = T(I_n) = (I_n)^T$ (by the definition of $T$). But Proposition 1.1 (b) (applied to $u = n$) yields $(I_n)^T = I_n$. Hence, $T(1_K) = (I_n)^T = I_n$. But the definition of the ring $K^{op}$ yields $1_{K^{op}} = 1_K = I_n$. Comparing the latter two equalities, we obtain $T(1_K) = 1_{K^{op}}$. This proves Claim 4.]

We have now proven all four Claims 1, 2, 3 and 4. Hence, $T$ is a ring homomorphism from $K$ to $K^{op}$ (by the definition of a ring homomorphism).

Let us next prove that the map $T$ is invertible. In proving this, we do not need to concern ourselves with the ring structures (i.e., the additions, multiplications, zeroes and unities) of $K$ and $K^{op}$, but can simply consider $K$ and $K^{op}$ as sets (because the invertibility of a map has nothing to do with any ring structures).

Recall that $K^{op} = K$ as sets. Thus, the map $T$ is a map from $K$ to $K$ (since $T$ is a map from $K$ to $K^{op}$). Hence, the map $T \circ T : K \to K$ is well-defined. Moreover, each $P \in K$ satisfies

\[
(T \circ T)(P) = T \left( \begin{pmatrix} T(P) \\ \end{pmatrix} \right) = T \left( P^T \right) = (P^T)^T \quad \text{(by the definition of } T) \]

\[
= P \quad \text{(by Proposition 1.1 (e) (applied to } u = n \text{ and } v = n) \}

\]

\[
= \text{id} \ (P) .
\]

In other words, $T \circ T = \text{id}$. Hence, the maps $T : K \to K$ and $T : K \to K$ are mutually inverse. Thus, the map $T : K \to K$ is invertible. In other words, the map $T : K \to K^{op}$ is invertible (since $K = K^{op}$ as sets).

So we have proven that the map $T : K \to K^{op}$ is an invertible ring homomorphism from $K$ to $K^{op}$. Thus, this map $T$ is a ring isomorphism from $K$ to $K^{op}$ (since any invertible ring homomorphism is a ring isomorphism). This solves part (c) of the exercise.

---

2 Exercise 2: More ring isomorphisms

2.1 Problem

(a) Let $L$ be a ring. Let $w \in L$ be an invertible element. Prove that the map $L \to L$, $a \mapsto awa^{-1}$ is a ring isomorphism.
(b) Let $\mathbb{K}$ be a ring. Let $W$ be the $n \times n$-matrix

$$(i + j = n + 1)_{1 \leq i \leq n, \ 1 \leq j \leq n} = \begin{pmatrix}
0 & \cdots & 0 & 1 \\
0 & \cdots & 0 & 1 \\
0 & \cdots & 1 & 0 \\
\vdots & \ddots & \vdots & \vdots \\
1 & \cdots & 0 & 0
\end{pmatrix} \in \mathbb{K}^{n \times n}$$

(where we are using the Iverson bracket notation again).
Prove that $W = W^{-1}$.

(c) Let $A = (a_{i,j})_{1 \leq i \leq n, \ 1 \leq j \leq n} \in \mathbb{K}^{n \times n}$ be any $n \times n$-matrix. Prove that

$$WAW^{-1} = (a_{n+1-i,n+1-j})_{1 \leq i \leq n, \ 1 \leq j \leq n}.$$

(In other words, $WAW^{-1}$ is the $n \times n$-matrix obtained from $A$ by reversing the order of the rows and also reversing the order of the columns.)

2.2 Remark
The map

$$\mathbb{L} \to \mathbb{L}, \quad a \mapsto waw^{-1}$$

in part (a) of this exercise is called conjugation by $w$. It is best known in the case of a matrix ring, where it corresponds to a change of basis for an endomorphism of a vector space. When $\mathbb{K}$ is a field, the only ring isomorphisms $\mathbb{K}^{n \times n} \to \mathbb{K}^{n \times n}$ are conjugations by invertible matrices; this is the Noether–Skolem theorem (in one of its less general variants).

2.3 Solution
(a) Let $f$ be the map

$$\mathbb{L} \to \mathbb{L}, \quad a \mapsto waw^{-1}.$$  

We must prove that $f$ is a ring isomorphism.

In class, we have proven that any invertible ring homomorphism is a ring isomorphism. Hence, it suffices to prove that $f$ is an invertible ring homomorphism.

Let us first prove that $f$ is a ring homomorphism. In order to do so, we need to verify the following four claims:

Claim 1: We have $f(a + b) = f(a) + f(b)$ for all $a, b \in \mathbb{L}$.

Claim 2: We have $f(0) = 0$.

Claim 3: We have $f(ab) = f(a)f(b)$ for all $a, b \in \mathbb{L}$.

Claim 4: We have $f(1) = 1$.

Let us now prove these claims:

Proof of Claim 1: Let $a, b \in \mathbb{L}$. The definition of $f$ yields $f(a) = waw^{-1}$ and $f(b) = wbw^{-1}$ and $f(a + b) = w(a + b)w^{-1}$. Hence,

$$f(a + b) = w \underbrace{(a + b)w^{-1}}_{= waw^{-1} + wbw^{-1} \quad \text{(by distributivity)}} = w \underbrace{(aw^{-1} + bw^{-1})}_{= f(a) + f(b) \quad \text{(by distributivity)}} = f(a) + f(b).$$
This proves Claim 1.

[Proof of Claim 2: The definition of \( f \) yields \( f(0) = w_0w^{-1}w_0 = 0 \). This proves \( =0 \).

Claim 2.]

[Proof of Claim 3: Let \( a, b \in \mathbb{L} \). The definition of \( f \) yields \( f(a) = waw^{-1} \) and \( f(b) = wbw^{-1} \). Hence,
\[
\begin{align*}
\frac{f(a)}{\text{by the definition of } f} \cdot \frac{f(b)}{\text{by the definition of } f} = waw^{-1}wbw^{-1} = wabw^{-1} = w(ab)w^{-1} = f(ab).
\end{align*}
\]
In other words, \( f(ab) = f(a)f(b) \). This proves Claim 3.]

[Proof of Claim 4: The definition of \( f \) yields \( f(1) = w_1w^{-1}w_1 = 1 \). This proves \( =_{w^{-1}} \).

We have now proven all four Claims 1, 2, 3 and 4. Hence, \( f \) is a ring homomorphism from \( \mathbb{L} \) to \( \mathbb{L} \) (by the definition of a ring homomorphism).

Let us next prove that the map \( f \) is invertible.

Indeed, let \( g \) be the map
\[
\mathbb{L} \to \mathbb{L}, \quad a \mapsto w^{-1}aw.
\]

Then, each \( a \in \mathbb{L} \) satisfies
\[
(g \circ f)(a) = g(f(a)) = w^{-1} \cdot \frac{f(a)}{\text{by the definition of } g} \cdot w = w^{-1}a^{-1}w = a = \text{id}(a).
\]

In other words, \( g \circ f = \text{id} \).

Also, each \( a \in \mathbb{L} \) satisfies
\[
(f \circ g)(a) = f(g(a)) = w \cdot \frac{g(a)}{\text{by the definition of } f} \cdot w^{-1} = w^{-1}aw = a = \text{id}(a).
\]

In other words, \( f \circ g = \text{id} \).

Now, the two maps \( f \) and \( g \) are mutually inverse (since \( f \circ g = \text{id} \) and \( g \circ f = \text{id} \)). Thus, the map \( f \) is invertible.

So we have proven that the map \( f \) is an invertible ring homomorphism. Thus, this map \( f \) is a ring isomorphism (since any invertible ring homomorphism is a ring isomorphism). This solves part (a) of the exercise.

(b) We first show two auxiliary claims about how multiplication by \( W \) changes a matrix:

Claim 5: Let \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathbb{K}^{n \times n} \) be any \( n \times n \)-matrix. Then,
\[
WA = (a_{n+1-i,j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

Claim 6: Let \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathbb{K}^{n \times n} \) be any \( n \times n \)-matrix. Then,
\[
AW = (a_{i,n+1-j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]
Proof of Claim 5: We have \( W = ([i + j = n + 1])_{1 \leq i \leq n, 1 \leq j \leq n} \) and \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \). Hence, the definition of the multiplication of matrices yields

\[
WA = \left( \sum_{k=1}^{n} [i + k = n + 1] a_{k,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

(5)

Now, let \( (i, j) \in \{1, 2, \ldots, n\}^2 \). Thus, \( i, j \in \{1, 2, \ldots, n\} \). From \( i \in \{1, 2, \ldots, n\} \), we obtain \( n + 1 - i \in \{1, 2, \ldots, n\} \). Now,

\[
\sum_{k=1}^{n} [i + k = n + 1] a_{k,j} = \sum_{k \in \{1, 2, \ldots, n\}} [i + k = n + 1] a_{k,j} = [i + (n + 1 - i) = n + 1] a_{n+1-i,j} + \sum_{k \in \{1, 2, \ldots, n\}; k \neq n+1-i} [i + k = n + 1] a_{k,j}
\]

(since \( i+(n+1-i)=n+1 \))

\[
= a_{n+1-i,j} + \sum_{k \in \{1, 2, \ldots, n\}; k \neq n+1-i} 0 a_{k,j} = a_{n+1-i,j}.
\]

(6)

Now, forget that we fixed \( (i, j) \). We thus have proven (6) for each \( (i, j) \in \{1, 2, \ldots, n\}^2 \). Thus, we have

\[
\left( \sum_{k=1}^{n} [i + k = n + 1] a_{k,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = (a_{n+1-i,j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

Hence, (6) becomes

\[
WA = \left( \sum_{k=1}^{n} [i + k = n + 1] a_{k,j} \right)_{1 \leq i \leq n, 1 \leq j \leq n} = (a_{n+1-i,j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

This proves Claim 5.

Proof of Claim 6: We have \( A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \) and \( W = ([i + j = n + 1])_{1 \leq i \leq n, 1 \leq j \leq n} \). Hence, the definition of the multiplication of matrices yields

\[
AW = \left( \sum_{k=1}^{n} a_{i,k} [k + j = n + 1] \right)_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

(7)

Now, let \( (i, j) \in \{1, 2, \ldots, n\}^2 \). Thus, \( i, j \in \{1, 2, \ldots, n\} \). From \( j \in \{1, 2, \ldots, n\} \), we
obtain \( n + 1 - j \in \{1, 2, \ldots, n\} \). Now,

\[
\sum_{k=1}^{n} a_{i,k} [k + j = n + 1] = \sum_{k \in \{1, 2, \ldots, n\}} a_{i,k} [k + j = n + 1] = a_{i,n+1-j} \left[ (n + 1 - j) + j = n + 1 \right] + \sum_{\substack{k \in \{1, 2, \ldots, n\}:
k \neq n+1-j}} a_{i,k} [k + j = n + 1] = a_{i,n+1-j} + \sum_{\substack{k \in \{1, 2, \ldots, n\}:
k \neq n+1-j}} a_{i,k}0 = a_{i,n+1-j}.
\]

Thus, we have

\[
\text{(8)}
\]

Hence, Claim 6.

Now, let \( n \in \mathbb{N} \). Namely, \( \delta_{i,j} \) yields

\[
A \delta_{i,j} \delta_{i,j} = \delta_{i,j} \delta_{i,j} W = \left( \sum_{k=1}^{n} a_{i,k} [k + j = n + 1] \right)_{1 \leq i \leq n, 1 \leq j \leq n} = \left( a_{i,n+1-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

Now, forget that we fixed \( (i, j) \). We thus have proven (8) for each \( (i, j) \in \{1, 2, \ldots, n\}^2 \). Thus, we have

\[
\left( \sum_{k=1}^{n} a_{i,k} [k + j = n + 1] \right)_{1 \leq i \leq n, 1 \leq j \leq n} = \left( a_{i,n+1-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

Hence, (8) becomes

\[
AW = \left( \sum_{k=1}^{n} a_{i,k} [k + j = n + 1] \right)_{1 \leq i \leq n, 1 \leq j \leq n} = \left( a_{i,n+1-j} \right)_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

This proves Claim 6.

Let us now come back to part (b) of this exercise. Recall the definition of the identity matrix \( I_n \in \mathbb{K}^{n \times n} \). Namely, \( I_n \) is defined by

\[
I_n = (\delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}, \quad \text{where } \delta_{i,j} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j. \end{cases}
\]

(Note that \( \delta_{i,j} \) can also be written as \( [i = j] \) using the Iverson bracket notation.)

Now, \( W = ([i + j = n + 1])_{1 \leq i \leq n, 1 \leq j \leq n} \). Hence, Claim 6 (applied to \( A = W \) and \( a_{i,j} = [i + j = n + 1] \)) yields

\[
WW = ([n + 1 - i + j = n + 1])_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

Now, let \( (i, j) \in \{1, 2, \ldots, n\}^2 \). Thus, \( i, j \in \{1, 2, \ldots, n\} \). Now, the statement “\( (n + 1 - i) + j = n + 1 \)” is equivalent to “\( i = j \)” (since \( (n + 1 - i) + j = (n + 1) = j - i \)). Thus,

\[
[(n + 1 - i) + j = n + 1] = [i = j] = \begin{cases} 1, & \text{if } i = j \text{ is true}; \\ 0, & \text{if } i = j \text{ is false} \end{cases}
\]

(by the definition of the Iverson bracket notation)

\[
= \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j \end{cases} = \delta_{i,j}.
\]

\[
(10)
\]
Forget that we fixed $(i,j)$. We thus have proven (10) for each $(i,j) \in \{1,2,\ldots,n\}^2$. Thus, we have

\[
((n+1-i) + j = n + 1)_{1 \leq i \leq n, 1 \leq j \leq n} = (\delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

Hence, (9) becomes

\[
WW = ((n+1-i) + j = n + 1)_{1 \leq i \leq n, 1 \leq j \leq n} = (\delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} = I_n.
\]

Now, the matrix $W$ is an inverse of $W$ (since $WW = I_n$ and $WW = I_n$). Thus, the matrix $W$ is invertible, and its inverse is $W^{-1} = W$. This solves part (b) of the exercise.

(c) We have $A = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$. Thus, Claim 5 yields

\[
WA = (a_{n+1-i,j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

Hence, Claim 6 (applied to $WA$ and $a_{n+1-i,j}$ instead of $A$ and $a_{i,j}$) yields

\[
WAW = (a_{n+1-i,n+1-j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

But part (b) of this exercise yields $W = W^{-1}$. Hence, $WA \underbrace{W}_{=W^{-1}} = WAW^{-1}$, so that

\[
WAW^{-1} = WAW = (a_{n+1-i,n+1-j})_{1 \leq i \leq n, 1 \leq j \leq n}.
\]

This solves part (c) of the exercise.

3 EXERCISE 3: ENTANGLED INVERSES

Let $\mathbb{K}$ be a ring.

A left inverse of an element $x \in \mathbb{K}$ is defined to be a $y \in \mathbb{K}$ such that $yx = 1$.

A right inverse of an element $x \in \mathbb{K}$ is defined to be a $y \in \mathbb{K}$ such that $xy = 1$.

Let $a$ and $b$ be two elements of $\mathbb{K}$. Prove the following:

(a) If $c$ is a left inverse of $1 - ab$, then $1 + bca$ is a left inverse of $1 - ba$.

(b) If $c$ is a right inverse of $1 - ab$, then $1 + bca$ is a right inverse of $1 - ba$.

(c) If $c$ is an inverse of $1 - ab$, then $1 + bca$ is an inverse of $1 - ba$.

Here and in the following, the word “inverse” (unless qualified with an adjective) means “multiplicative inverse”.

3.1 SOLUTION

(a) Assume that $c$ is a left inverse of $1 - ab$. Thus, $c(1 - ab) = 1$ (by the definition of a left inverse).
Now, the laws of distributivity\(^2\) yield
\[ a (1 - ba) = a - aba = (1 - ab) a, \]
thus
\[ c a (1 - ba) = c (1 - ab) a = 1a = a. \]

Hence, using the distributivity axiom, we obtain
\[ (1 + bca) (1 - ba) = (1 - ba) + bca (1 - ba) = (1 - ba) + ba = 1. \]

In other words, \(1 + bca\) is a left inverse of \(1 - ba\) (by the definition of a left inverse). This solves part (a) of the exercise.

(b) Assume that \(c\) is a right inverse of \(1 - ab\). Thus, \((1 - ab) c = 1\) (by the definition of a right inverse).

Now, the laws of distributivity yield
\[ (1 - ba) b = b - bab = b (1 - ab), \]
thus
\[ (1 - ba) b c = b (1 - ab) c = b1 = b. \]

Hence, using the distributivity axiom, we obtain
\[ (1 - ba) (1 + bca) = (1 - ba) + (1 - ba) bc a = (1 - ba) + ba = 1. \]

In other words, \(1 + bca\) is a right inverse of \(1 - ba\) (by the definition of a right inverse). This solves part (b) of the exercise.

(c) Assume that \(c\) is an inverse of \(1 - ab\). In other words, \(c\) is a multiplicative inverse of \(1 - ab\). Thus, \((1 - ab) c = c (1 - ab) = 1\) (by the definition of a multiplicative inverse).

From \(c (1 - ab) = 1\), we conclude that \(c\) is a left inverse of \(1 - ab\). Hence, part (a) of this exercise shows that \(1 + bca\) is a left inverse of \(1 - ba\). In other words, \((1 + bca) (1 - ba) = 1\).

From \((1 - ab) c = 1\), we conclude that \(c\) is a right inverse of \(1 - ab\). Hence, part (b) of this exercise shows that \(1 + bca\) is a right inverse of \(1 - ba\). In other words, \((1 - ba) (1 + bca) = 1\).

Combining \((1 + bca) (1 - ba) = 1\) with \((1 - ba) (1 + bca) = 1\), we obtain \((1 - ba) (1 + bca) = (1 + bca) (1 - ba) = 1\). In other words, \(1 + bca\) is a multiplicative inverse of \(1 - ab\) (by the definition of a multiplicative inverse). In other words, \(1 + bca\) is an inverse of \(1 - ab\). This solves part (c) of the exercise.

---

\(^2\)When we say “the laws of distributivity” here, we mean not just the axiom of distributivity (which says that \(u (v + w) = uv + uw\) and \((u + v) w = uw + vw\) for all \(u, v, w \in K\)), but also its analogue for subtraction (which says that \(u (v - w) = uv - uw\) and \((u - v) w = uw - vw\) for all \(u, v, w \in K\)). The latter analogue is not one of the ring axioms, but follows easily from them.
4 Exercise 4: Composition of ring homomorphisms

4.1 Problem

Let \( K, L \) and \( M \) be three rings. Prove the following:

(a) If \( f : K \to L \) and \( g : L \to M \) are two ring homomorphisms, then \( g \circ f : K \to M \) is a ring homomorphism.

(b) If \( f : K \to L \) and \( g : L \to M \) are two ring isomorphisms, then \( g \circ f : K \to M \) is a ring isomorphism.

4.2 Solution

(a) Let \( f : K \to L \) and \( g : L \to M \) be two ring homomorphisms. We must prove that \( g \circ f : K \to M \) is a ring homomorphism.

We have assumed that \( f : K \to L \) is a ring homomorphism. In other words, \( f \) satisfies the four axioms in our definition of a ring homomorphism. In other words, the following four claims hold:

Claim 1: We have \( f (a + b) = f (a) + f (b) \) for all \( a, b \in K \).

Claim 2: We have \( f (0) = 0 \).

Claim 3: We have \( f (ab) = f (a) f (b) \) for all \( a, b \in K \).

Claim 4: We have \( f (1) = 1 \).

Similarly, from the assumption that \( g : L \to M \) is a ring homomorphism, we conclude that the following four claims hold:

Claim 5: We have \( g (a + b) = g (a) + g (b) \) for all \( a, b \in L \).

Claim 6: We have \( g (0) = 0 \).

Claim 7: We have \( g (ab) = g (a) g (b) \) for all \( a, b \in L \).

Claim 8: We have \( g (1) = 1 \).

Now, we must prove that \( g \circ f : K \to M \) is a ring homomorphism. In other words, we must prove that \( g \circ f \) satisfies the four axioms in our definition of a ring homomorphism. In other words, we must prove that the following four claims hold:

Claim 9: We have \( (g \circ f) (a + b) = (g \circ f) (a) + (g \circ f) (b) \) for all \( a, b \in K \).

Claim 10: We have \( (g \circ f) (0) = 0 \).

Claim 11: We have \( (g \circ f) (ab) = (g \circ f) (a) (g \circ f) (b) \) for all \( a, b \in K \).

Claim 12: We have \( (g \circ f) (1) = 1 \).
But this is straightforward:

[Proof of Claim 9: For all \(a, b \in K\), we have

\[
(g \circ f)(a + b) = g \left( f(a + b) \right) = g(f(a) + f(b)) = g(f(a)) + g(f(b))
\]

(by Claim 5, applied to \(f(a)\) and \(f(b)\) instead of \(a\) and \(b\))

\[
= (g \circ f)(a) + (g \circ f)(b)
\]

Thus, Claim 9 is proven.]

[Proof of Claim 10: We have \((g \circ f)(0) = g(f(0)) = 0\) (by Claim 6).

Thus, Claim 10 is proven.]

[Proof of Claim 11: The proof of Claim 11 is analogous to the proof of Claim 9, except that we need to use Claims 3 and 7 instead of Claims 1 and 5.]

[Proof of Claim 12: The proof of Claim 12 is analogous to the proof of Claim 10, except that we need to use Claims 4 and 8 instead of Claims 2 and 6.]

Thus, all four Claims 9, 10, 11 and 12 are proven. As we explained, this shows that \(g \circ f\) is a ring homomorphism. Hence, part (a) of the exercise is solved.

(b) Let \(f : K \to L\) and \(g : L \to M\) be two ring isomorphisms. We must show that \(g \circ f: K \to M\) is a ring isomorphism.

The map \(f\) is a ring isomorphism. In other words, \(f\) is invertible and both \(f\) and \(f^{-1}\) are ring homomorphisms (by the definition of a ring isomorphism).

The map \(g\) is a ring isomorphism. In other words, \(g\) is invertible and both \(g\) and \(g^{-1}\) are ring homomorphisms (by the definition of a ring isomorphism).

Now we know that \(f : K \to L\) and \(g : L \to M\) are two ring homomorphisms. Hence, part (a) of this exercise shows that \(g \circ f : K \to M\) is a ring homomorphism.

Also, we know that \(g^{-1} : M \to L\) and \(f^{-1} : L \to K\) are two ring homomorphisms. Hence, part (a) of this exercise (applied to \(M, K, g^{-1}\) and \(f^{-1}\) instead of \(K, M, f\) and \(g\)) shows that \(f^{-1} \circ g^{-1} : M \to K\) is a ring homomorphism.

But the maps \(f\) and \(g\) are invertible. Hence, it is well-known that their composition \(g \circ f\) is invertible as well, and its inverse is \((g \circ f)^{-1} = f^{-1} \circ g^{-1}\). Hence, \((g \circ f)^{-1}\) is a ring homomorphism (since \(f^{-1} \circ g^{-1}\) is a ring homomorphism).

Now, we know that the map \(g \circ f\) is invertible and both \(g \circ f\) and \((g \circ f)^{-1}\) are ring homomorphism. In other words, \(g \circ f\) is a ring isomorphism (by the definition of a ring isomorphism). This solves part (b) of the exercise.

5 Exercise 5: Squares in finite fields I

5.1 Problem

Let \(F\) be a field.
(a) Prove that if \( a, b \in F \) satisfy \( ab = 0 \), then \( a = 0 \) or \( b = 0 \).

(b) Prove that if \( a, b \in F \) satisfy \( a^2 = b^2 \), then \( a = b \) or \( a = -b \).

Recall that an element \( \eta \in F \) is called a \textit{square} if there exists some \( \alpha \in F \) such that \( \eta = \alpha^2 \).

From now on, assume that \( 2 \cdot 1_F \neq 0_F \) (that is, \( 1_F + 1_F \neq 0_F \)). Note that this is satisfied whenever \( F = \mathbb{Z}/p \) for a prime \( p > 2 \) (but also for various other finite fields), but fails when \( F = \mathbb{Z}/2 \).

(c) Prove that \( a \neq -a \) for every nonzero \( a \in F \).

From now on, assume that \( F \) is finite.

d) Prove that the number of squares in \( F \) is \( \frac{1}{2} (|F| + 1) \).

(e) Conclude that \( |F| \) is odd.

[Hint: For part (d), argue that each nonzero square in \( F \) can be written as \( \alpha^2 \) for exactly two \( \alpha \in F \).]

### 5.2 Solution

We have assumed that \( F \) is a field. Hence, \( F \) is a commutative skew field (by the definition of a field). Every nonzero element of \( F \) is invertible (since \( F \) is a skew field).

(a) Let \( a, b \in F \) be such that \( ab = 0 \). We must prove that \( a = 0 \) or \( b = 0 \).

Assume the contrary. Thus, neither \( a = 0 \) nor \( b = 0 \) holds. In other words, we have \( a \neq 0 \) and \( b \neq 0 \). Thus, the elements \( a \) and \( b \) of \( F \) are nonzero, and therefore invertible (since every nonzero element of \( F \) is invertible). Hence, their inverses \( a^{-1} \) and \( b^{-1} \) are well-defined. Comparing the equalities \( a^{-1}ab = b \) and \( a^{-1}ab = a^{-1}0 = 0 \), we obtain \( b = 0 \). This contradicts \( b \neq 0 \). This contradiction shows that our assumption was false. This completes the solution to part (a) of the exercise.

(b) Let \( a, b \in F \) satisfy \( a^2 = b^2 \). We must prove that \( a = b \) or \( a = -b \).

Since \( F \) is commutative, we have \( ab = ba \). Now, multiplying out \( (a - b)(a + b) \) (by applying the distributivity laws several times), we obtain

\[
(a - b)(a + b) = \frac{aa}{a^2 = b^2} + \frac{ab}{ab} - \frac{ba}{ba} - \frac{bb}{b^2} = b^2 + ba - ba - b^2 = 0.
\]

Thus, part (a) of this exercise (applied to \( a - b \) and \( a + b \) instead of \( a \) and \( b \)) shows that \( a - b = 0 \) or \( a + b = 0 \). In other words, \( a = b \) or \( a = -b \). Thus, part (b) of the exercise is solved.

(c) Let \( a \in F \) be nonzero. We must prove that \( a \neq -a \).

Assume the contrary. Thus, \( a = -a \), so that \( a + a = 0 \). Now,

\[
\underbrace{(2 \cdot 1_F)}_{=1_F + 1_F} a = (1_F + 1_F) a = 1_F a + 1_F a = a + a = 0.
\]

Darij Grinberg, 00000000
dgrinber@umn.edu
The element $2 \cdot 1_\mathbb{F}$ of $\mathbb{F}$ is nonzero (since $2 \cdot 1_\mathbb{F} \neq 0_\mathbb{F}$), and thus invertible (since every nonzero element of $\mathbb{F}$ is invertible). Hence, it has a well-defined inverse $(2 \cdot 1_\mathbb{F})^{-1}$.

Now,

$$(2 \cdot 1_\mathbb{F})^{-1} \cdot (2 \cdot 1_\mathbb{F}) a = (2 \cdot 1_\mathbb{F})^{-1} \cdot 0 = 0.$$ 

Comparing this with $(2 \cdot 1_\mathbb{F})^{-1} \cdot (2 \cdot 1_\mathbb{F}) a = 1 a = a$, we obtain $a = 0$. This contradicts the fact that $a$ is nonzero. This contradiction shows that our assumption was false. Hence, $a \neq -a$. Thus, part (c) of the exercise is solved.

(d) We have the following:

Claim 1: Let $c \in \mathbb{F}$. Then:

(i) If $c$ is a nonzero square, then

$$\left| \{d \in \mathbb{F} \mid c = d^2 \} \right| = 2.$$ 

(ii) If $c$ is not a square, then

$$\left| \{d \in \mathbb{F} \mid c = d^2 \} \right| = 0.$$ 

(iii) If $c = 0$, then

$$\left| \{d \in \mathbb{F} \mid c = d^2 \} \right| = 1.$$ 

Proof of Claim 1: (i) Assume that $c$ is a nonzero square. Thus, there exists a $g \in \mathbb{F}$ such that $c = g^2$ (since $c$ is a square). Consider this $g$. Moreover,

$$(g)^2 = (g)(g) = -(g \cdot g) = -(gg) = gg = g^2 = c.$$ 

(since $c = g^2$). Hence, $c = (g)^2$.

If we had $g = 0$, then we would have $c = 0^2 = 0^2 = 0$, which would contradict our assumption that $c$ is nonzero. Hence, we cannot have $g = 0$. Thus, $g$ is nonzero. Therefore, $g \neq -g$ (by part (c) of this exercise, applied to $a = g$). Hence, the elements $g$ and $-g$ of $\mathbb{F}$ are distinct. Thus, $\left| \{g, -g\} \right| = 2$.

But $g \in \{d \in \mathbb{F} \mid c = d^2 \}$ (since $g \in \mathbb{F}$ and $c = g^2$) and $-g \in \{d \in \mathbb{F} \mid c = d^2 \}$ (since $-g \in \mathbb{F}$ and $c = (-g)^2$). Combining these two facts, we obtain

$$\{g, -g\} \subseteq \{d \in \mathbb{F} \mid c = d^2 \}.$$  \hspace{1cm} (11)

On the other hand, let us prove that $\{d \in \mathbb{F} \mid c = d^2 \} \subseteq \{g, -g\}$. Indeed, let $a \in \{d \in \mathbb{F} \mid c = d^2 \}$. Thus, $a$ is a $d \in \mathbb{F}$ such that $c = d^2$. In other words, $a$ is an element of $\mathbb{F}$ and satisfies $c = a^2$. Hence, $a^2 = c = g^2$. Thus, part (b) of this exercise (applied to $b = g$) yields that $a = g$ or $a = -g$. In other words, $a \in \{g, -g\}$. Now, forget that we fixed $a$. We thus have shown that $a \in \{g, -g\}$ for each $a \in \{d \in \mathbb{F} \mid c = d^2 \}$. In other words, 

$$\{d \in \mathbb{F} \mid c = d^2 \} \subseteq \{g, -g\}.$$ 

Combining this with (11), we obtain

$$\{d \in \mathbb{F} \mid c = d^2 \} = \{g, -g\}.$$ 

Hence,

$$\left| \{d \in \mathbb{F} \mid c = d^2 \} \right| = \left| \{g, -g\} \right| = 2.$$
This proves Claim 1 (i).

(ii) Assume that $c$ is not a square. Then, there exists no $\alpha \in \mathbb{F}$ such that $c = \alpha^2$ (by the definition of a square). In other words, there exists no $d \in \mathbb{F}$ such that $c = d^2$ (here, we have renamed the index $\alpha$ as $d$). In other words, $\{d \in \mathbb{F} \mid c = d^2\} = \emptyset$. Hence, $|\{d \in \mathbb{F} \mid c = d^2\}| = |\emptyset| = 0$. This proves Claim 1 (ii).

(iii) Assume that $c = 0$. Then, $0 \in \{d \in \mathbb{F} \mid c = d^2\}$ (since $g \in \mathbb{F}$ and $c = 0 = 0^2$) and thus $\{0\} \subseteq \{d \in \mathbb{F} \mid c = d^2\}$.

On the other hand, let us show that $\{d \in \mathbb{F} \mid c = d^2\} \subseteq \{0\}$.

Indeed, let $a \in \{d \in \mathbb{F} \mid c = d^2\}$. Then, $a$ is a $d \in \mathbb{F}$ such that $c = d^2$. In other words, $a$ is an element of $\mathbb{F}$ and satisfies $c = a^2$. Hence, $aa = a^2 = c = 0$. Thus, part (a) of this exercise (applied to $b = a$) yields that $a = 0$ or $a = 0$. In other words, $a = 0$. In other words, $a \in \{0\}$. Now, forget that we fixed $a$. We thus have shown that $a \in \{0\}$ for each $a \in \{d \in \mathbb{F} \mid c = d^2\}$. In other words, $\{d \in \mathbb{F} \mid c = d^2\} \subseteq \{0\}$. Combining this with $\{0\} \subseteq \{d \in \mathbb{F} \mid c = d^2\}$, we obtain $\{d \in \mathbb{F} \mid c = d^2\} = \{0\}$. Hence, $|\{d \in \mathbb{F} \mid c = d^2\}| = |\{0\}| = 1$. This proves Claim 1 (iii).]

Now, let us count all pairs $(c, d) \in \mathbb{F} \times \mathbb{F}$ satisfying $c = d^2$. We shall count these pairs in two ways:

- The first way is to split this count according to the value of $c$ (that is, first count all such pairs $(c, d)$ with a given $c$, and then sum the result up over all $c \in \mathbb{F}$). Thus, we find

\[
\begin{align*}
\text{(the number of all } & (c, d) \in \mathbb{F} \times \mathbb{F} \text{ such that } c = d^2) \\
= & \sum_{c \in \mathbb{F}} \left( \text{(the number of all } d \in \mathbb{F} \text{ such that } c = d^2) \right) \\
= & \sum_{c \in \mathbb{F}} \left| \{d \in \mathbb{F} \mid c = d^2\} \right| \\
= & \sum_{c \in \mathbb{F}} \left( \sum_{\substack{d \in \mathbb{F} : \\ c = d^2}} 1 \right) + \sum_{c \in \mathbb{F} : c \text{ is a nonzero square}} 2 \left( \text{by Claim 1 (iii)} \right) + \sum_{c \in \mathbb{F} : c \text{ is not a square}} 0 \left( \text{by Claim 1 (i)} \right) \\
= & \sum_{c \in \mathbb{F} : c = 0} 1 + \sum_{c \in \mathbb{F} : c \text{ is a nonzero square}} 2 + \sum_{c \in \mathbb{F} : c \text{ is not a square}} 0 \\
= & 1 + 2 \cdot (\text{the number of nonzero squares in } \mathbb{F}) + 0 \\
= & 1 + 2 \cdot (\text{the number of nonzero squares in } \mathbb{F}).
\end{align*}
\]

- The second way is to split this count according to the value of $d$ (that is, first count all such pairs $(c, d)$ with a given $d$, and then sum the result up over all $d \in \mathbb{F}$). Thus,
we find
\[
(\text{the number of all } (c, d) \in \mathbb{F} \times \mathbb{F} \text{ such that } c = d^2) \\
= \sum_{d \in \mathbb{F}} (\text{the number of all } c \in \mathbb{F} \text{ such that } c = d^2) \\
(\text{since there is exactly one } c \in \mathbb{F} \text{ such that } c = d^2 \text{ (namely, } c = d^2)) \\
= \sum_{d \in \mathbb{F}} 1 = |\mathbb{F}| \cdot 1 = |\mathbb{F}|.
\]

Comparing these two equalities, we obtain
\[
|\mathbb{F}| = 1 + 2 \cdot (\text{the number of nonzero squares in } \mathbb{F}).
\]

Solving this for (the number of nonzero squares in \(\mathbb{F}\)), we find
\[
(\text{the number of nonzero squares in } \mathbb{F}) = \frac{|\mathbb{F}| - 1}{2}.
\]

Now, there are two kinds of squares in \(\mathbb{F}\): namely, the nonzero squares (of which there are exactly \(\frac{|\mathbb{F}| - 1}{2}\) many, as we just proved) and the zero squares (of which there is only 1, namely \(0^2 = 0\)). Thus, the total number of squares in \(\mathbb{F}\) is
\[
\frac{|\mathbb{F}| - 1}{2} + 1 = \frac{|\mathbb{F}| + 1}{2} = \frac{1}{2} (|\mathbb{F}| + 1).
\]
This solves part (d) of the exercise.

(e) Part (d) of this exercise shows that the number of squares in \(\mathbb{F}\) is \(\frac{1}{2} (|\mathbb{F}| + 1)\). Thus,
\[
\frac{1}{2} (|\mathbb{F}| + 1) = (\text{the number of squares in } \mathbb{F}) \in \mathbb{N}
\]
(since a number that counts something is always \(\in \mathbb{N}\)). Therefore, \(\frac{1}{2} (|\mathbb{F}| + 1) \in \mathbb{N} \subseteq \mathbb{Z}\), so that the integer \(|\mathbb{F}| + 1\) is even. This shows that \(|\mathbb{F}|\) is odd. This solves part (e) of the exercise.

---

6 Exercise 6: The characteristic of a field

6.1 Problem

Let \(\mathbb{F}\) be a field. Recall that we have defined \(na\) to mean \(a + a + \cdots + a\) whenever \(n \in \mathbb{N}\) and \(a \in \mathbb{F}\).

Assume that there exists a positive integer \(n\) such that \(n \cdot 1_\mathbb{F} = 0\). Let \(p\) be the smallest such \(n\).

Prove that \(p\) is prime.

[Hint: \((a \cdot 1_\mathbb{F}) \cdot (b \cdot 1_\mathbb{F}) = ab \cdot 1_\mathbb{F}\) for all \(a, b \in \mathbb{N}\).]
6.2 REMARK

The $p$ we just defined is called the characteristic of the field $\mathbb{F}$ when it exists. (Otherwise, the characteristic of the field $\mathbb{F}$ is defined to be 0.)

Thus, for each prime $p$, the finite field $\mathbb{Z}/p$, as well as the finite field of size $p^2$ that we constructed in class, have characteristic $p$.

6.3 SOLUTION SKETCH

We have assumed that $\mathbb{F}$ is a field. Hence, $\mathbb{F}$ is a commutative skew field (by the definition of a field). We have $0_\mathbb{F} \neq 1_\mathbb{F}$ (since $\mathbb{F}$ is a skew field).

We have defined $p$ to be the smallest positive integer $n$ such that $n \cdot 1_\mathbb{F} = 0$. Thus, $p$ is a positive integer which itself satisfies $p \cdot 1_\mathbb{F} = 0$. Furthermore, if $n$ is a positive integer such that $n \cdot 1_\mathbb{F} = 0$, then

$$n \geq p$$

(since $p$ is the smallest positive integer $n$ such that $n \cdot 1_\mathbb{F} = 0$).

If we had $p = 1$, then we would have $p \cdot 1_\mathbb{F} = 1 \cdot 1_\mathbb{F} = 1_\mathbb{F} \neq 0_\mathbb{F}$ (since $0_\mathbb{F} \neq 1_\mathbb{F}$), which would contradict $p \cdot 1_\mathbb{F} = 0 = 0_\mathbb{F}$. Thus, we cannot have $p = 1$. Therefore, we have $p > 1$ (since $p$ is a positive integer).

We shall now show that the only positive divisors of $p$ are 1 and $p$. Indeed, assume the contrary. Thus, $p$ has a positive divisor other than 1 and $p$. Consider such a divisor, and denote it by $d$. Thus, $d$ is a positive divisor of $p$ that is distinct from 1 and $p$. In other words, $d$ is a positive divisor of $p$ and satisfies $d \neq 1$ and $d \neq p$. We have $d \leq p$ (since $d$ is a positive divisor of the prime integer $p$). Combining this with $d \neq p$, we obtain $d < p$. Also, $d \in \mathbb{Z}$ (since $d$ is an integer) and $d \neq p \in \mathbb{Z}$ (since $d$ is a divisor of $p$).

Now, for all $a, b \in \mathbb{Z}$, we have

$$(a \cdot 1_\mathbb{F}) \cdot (b \cdot 1_\mathbb{F}) = a \cdot (1_\mathbb{F} \cdot (b \cdot 1_\mathbb{F})) = a \cdot (b \cdot 1_\mathbb{F}) = ab \cdot 1_\mathbb{F}.$$  

Applying this to $a = d$ and $b = \frac{p}{d}$, we obtain

$$(d \cdot 1_\mathbb{F}) \cdot \left(\frac{p}{d} \cdot 1_\mathbb{F}\right) = d \cdot \frac{p}{d} \cdot 1_\mathbb{F} = p \cdot 1_\mathbb{F} = 0.$$  

Thus, Exercise 5 (a) (applied to $a = d \cdot 1_\mathbb{F}$ and $b = \frac{p}{d} \cdot 1_\mathbb{F}$) shows that $d \cdot 1_\mathbb{F} = 0$ or $\frac{p}{d} \cdot 1_\mathbb{F} = 0$.

If we had $d \cdot 1_\mathbb{F} = 0$, then we would have $d \geq p$ (by (12), applied to $n = d$), which would contradict $d < p$. Hence, we cannot have $d \cdot 1_\mathbb{F} = 0$. Thus, we have $\frac{p}{d} \cdot 1_\mathbb{F} = 0$ (since $d \cdot 1_\mathbb{F} = 0$ or $\frac{p}{d} \cdot 1_\mathbb{F} = 0$). But $\frac{p}{d}$ is an integer (since $\frac{p}{d} \in \mathbb{Z}$) and is positive (since $p$ and $d$ are positive); thus, $\frac{p}{d}$ is a positive integer. Hence, (12) (applied to $n = \frac{p}{d}$) yields $\frac{p}{d} \geq p$ (since $\frac{p}{d} \cdot 1_\mathbb{F} = 0$).

Since $d$ is positive, we can multiply this inequality by $d$, and thus obtain $p \geq pd$. Since $p$ is positive, we can divide this inequality by $p$, and thus obtain $1 \geq d$. Hence, $d = 1$ (since $d$ is a positive integer). This contradicts $d \neq 1$.

This contradiction shows that our assumption was false. Hence, the only positive divisors of $p$ are 1 and $p$. Thus, $p$ is a prime (since $p$ is an integer satisfying $p > 1$). Qed.
6.4 Remark

We have never used the commutativity of multiplication (in $F$) in the above proof. Thus, we can replace “field” by “skew field” in this exercise.

References


The numbering of theorems and formulas in this link might shift when the project gets updated; for a “frozen” version whose numbering is guaranteed to match that in the citations above, see https://github.com/darijgr/detnotes/releases/tag/2019-01-10.