Drexel University, Department of Mathematics

Math 533: Abstract Algebra I, Winter 2021: Homework 2

Version with solutions

Darij Grinberg

June 7, 2023

Contents

1 Exercise 1

1.1 Problem

Let R be a ring. Let a be a nilpotent element of R. (Recall that "nilpotent" means that there exists some $n \in \mathbb{N}$ such that $a^n = 0$.)

(a) Prove that $1 - a \in R$ is a unit.

(b) Let $u \in R$ be a unit satisfying $ua = au$. Prove that $u - a \in R$ is a unit.

[**Hint:** Treat the geometric series $\dfrac{1}{1-x} = 1 + x + x^2 + \cdots$ as an inspiration. Nilpotent elements of a ring are an algebraic analogue of the infamous "sufficiently small $\varepsilon > 0$" from real analysis. In particular, a nilpotent element a can be substituted (for x) into any formal power series $r_0 + r_1 x + r_2 x^2 + \cdots$, since the resulting sum will have only finitely many addends distinct from 0. (You don't actually need to write any infinite sums in your solution, but they can help you come up with the solution in the first place.)]

1.2 Solution

The element a of R is nilpotent. In other words, there exists some $n \in \mathbb{N}$ such that $a^n = 0$ (by the definition of "nilpotent"). Consider this n.

If u and v are two commuting elements[1] of R, then

$$u^m v = v u^m \qquad \text{for each } m \in \mathbb{N} \tag{1}$$

and

$$(uv)^m = u^m v^m \qquad \text{for each } m \in \mathbb{N}. \tag{2}$$

These are two known facts, which can both be proved by induction on m. For the sake of completeness, let me show the proofs:

[*Proof of (1):* We induct on m:

Induction base: Comparing $\underbrace{u^0}_{=1} v = 1v = v$ with $v \underbrace{u^0}_{=1} = v \cdot 1 = v$, we obtain $u^0 v = v u^0$. In other words, (1) holds for $m = 0$.

Induction step: Let $k \in \mathbb{N}$. Assume that (1) holds for $m = k$. We must show that (1) holds for $m = k+1$.

We have assumed that (1) holds for $m = k$. In other words, $u^k v = v u^k$. On the other hand, $uv = vu$ (since u and v are commuting). Now, $\underbrace{u^{k+1}}_{=uu^k} v = u \underbrace{u^k v}_{=vu^k} = \underbrace{uv}_{=vu} u^k = v \underbrace{uu^k}_{=u^{k+1}} = vu^{k+1}$. In other words, (1) holds for $m = k+1$. This completes the induction step. Thus, (1) is proven.]

[*Proof of (2):* We induct on m:

Induction base: Comparing $(uv)^0 = 1$ with $\underbrace{u^0}_{=1} \underbrace{v^0}_{=1} = 1 \cdot 1 = 1$, we obtain $(uv)^0 = u^0 v^0$. In other words, (2) holds for $m = 0$.

Induction step: Let $k \in \mathbb{N}$. Assume that (2) holds for $m = k$. We must show that (2) holds for $m = k+1$.

We have assumed that (2) holds for $m = k$. In other words, $(uv)^k = u^k v^k$. On the other hand, $u^k v = v u^k$ (by (1), applied to $m = k$). Now,

$$(uv)^{k+1} = (uv) \underbrace{(uv)^k}_{=u^k v^k} = (uv)\, u^k v^k = u \underbrace{v u^k}_{\substack{=u^k v \\ (\text{since } u^k v = v u^k)}} v^k = \underbrace{uu^k}_{=u^{k+1}} \underbrace{vv^k}_{=v^{k+1}} = u^{k+1} v^{k+1}.$$

In other words, (2) holds for $m = k+1$. This completes the induction step. Thus, (2) is proven.]

Now, we can step to the solution of the exercise:

(a) Define $b \in R$ by $b = a^0 + a^1 + \cdots + a^{n-1}$. Then,

$$\begin{aligned}
(1-a)\, b &= (1-a)\left(a^0 + a^1 + \cdots + a^{n-1}\right) \\
&= \underbrace{\left(a^0 + a^1 + \cdots + a^{n-1}\right)}_{=(a^0+a^1+\cdots+a^n)-a^n} - \underbrace{a\left(a^0 + a^1 + \cdots + a^{n-1}\right)}_{\substack{=aa^0+aa^1+\cdots+aa^{n-1} \\ =a^1+a^2+\cdots+a^n \\ =\left(a^0+a^1+\cdots+a^n\right)-a^0}} \\
&= \left(\left(a^0 + a^1 + \cdots + a^n\right) - a^n\right) - \left(\left(a^0 + a^1 + \cdots + a^n\right) - a^0\right) \\
&= \underbrace{a^0}_{=1} - \underbrace{a^n}_{=0} = 1 - 0 = 1
\end{aligned}$$

[1] Recall that two elements u and v of R are said to *commute* if $uv = vu$.

and

$$\begin{aligned} b\left(1-a\right) &= \left(a^0+a^1+\cdots+a^{n-1}\right)\left(1-a\right) \\ &= \underbrace{\left(a^0+a^1+\cdots+a^{n-1}\right)}_{=(a^0+a^1+\cdots+a^n)-a^n} - \underbrace{\left(a^0+a^1+\cdots+a^{n-1}\right)a}_{\substack{=a^0a+a^1a+\cdots+a^{n-1}a \\ =a^1+a^2+\cdots+a^n \\ =\left(a^0+a^1+\cdots+a^n\right)-a^0}} \\ &= \left(\left(a^0+a^1+\cdots+a^n\right)-a^n\right) - \left(\left(a^0+a^1+\cdots+a^n\right)-a^0\right) \\ &= \underbrace{a^0}_{=1} - \underbrace{a^n}_{=0} = 1-0=1. \end{aligned}$$

Combining these two equalities, we see that b is an inverse to $1-a$ in R. Hence, the element $1-a$ of R has an inverse, i.e., is a unit of R. This solves part **(a)** of the exercise.

(b) The element u is a unit of R, and thus has an inverse u^{-1}. This inverse u^{-1} satisfies $u^{-1}a = au^{-1}$ (this can be seen by comparing $u^{-1}\underbrace{ua}_{=au}u^{-1} = u^{-1}a\underbrace{uu^{-1}}_{=1} = u^{-1}a$ with $\underbrace{u^{-1}u}_{=1}au^{-1} = au^{-1}$). In other words, the two elements u^{-1} and a of R are commuting. Hence, (2) (applied to u^{-1}, a and n instead of u, v and m) yields $\left(u^{-1}a\right)^n = \left(u^{-1}\right)^n\underbrace{a^n}_{=0} = 0$. Hence, the element $u^{-1}a$ of R is nilpotent. Thus, we can apply part **(a)** of this exercise to $u^{-1}a$ instead of a. As a result, we conclude that $1-u^{-1}a \in R$ is a unit.

Now, recall that the units of R form a group under multiplication. Thus, the product of any two units of R is again a unit. Hence, the product $u\left(1-u^{-1}a\right)$ of u and $1-u^{-1}a$ is a unit (since u and $1-u^{-1}a$ are units). In other words, $u-a$ is a unit (since $u\left(1-u^{-1}a\right) = u-\underbrace{uu^{-1}}_{=1}a = u-a$). This solves part **(b)** of the exercise.

1.3 Remark

Our above solution carefully hides any traces of its origins, but they are still not hard to see: The $a^0+a^1+\cdots+a^{n-1}$ in the solution of part **(a)** is just the infinite sum $1+a+a^2+\cdots$ suggested by the hint, rewritten as a finite sum because $a^n=0$ renders all but the first n of its terms equal to 0.

The inverse of $u-a$ in part **(b)** of the exercise can also be written explicitly: It is $u^{-1}\left(\left(u^{-1}a\right)^0+\left(u^{-1}a\right)^1+\cdots+\left(u^{-1}a\right)^{n-1}\right)$.

The "$ua=au$" condition in part **(b)** cannot be dropped. For example, if u and a are the elements $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ of the matrix ring $\mathbb{Q}^{2\times 2}$, then u is a unit and a is nilpotent, but $u-a = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ is not invertible (i.e., not a unit of this matrix ring).

---

2 Exercise 2

2.1 Problem

Let R be a ring. We define a new binary operation $\widetilde{\cdot}$ on R by setting

$$a\mathbin{\widetilde{\cdot}}b = ba \qquad \text{for all } a,b \in R.$$

(Thus, $\mathbin{\widetilde{\cdot}}$ is the multiplication of R, but with the arguments switched.)

(a) Prove that the set R, equipped with the addition $+$, the multiplication $\mathbin{\widetilde{\cdot}}$, the zero 0_R and the unity 1_R, is a ring.

This new ring is called the *opposite ring* of R, and is denoted by R^{op}.

Note that the **sets** R and R^{op} are identical (so a map from R to R is the same as a map from R to R^{op}); but the **rings** R and R^{op} are generally not the same (so a ring morphism from R to R is not the same as a ring morphism from R to R^{op}).

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

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

$$R \to R^{\mathrm{op}}, \qquad A \mapsto A^T$$

(where A^T, as usual, denotes the transpose of a matrix A) is a ring isomorphism.

(d) Forget about S, and let R be an arbitrary ring again. Let M be a right R-module. Prove that M becomes a left R^{op}-module if we define an action of R^{op} on M by

$$rm = mr \qquad \text{for all } r \in R^{\mathrm{op}} \text{ and } m \in M.$$

(Here, the left hand side is to be understood as the image of (r, m) under the new action of R^{op} on M, whereas the right hand side is the image of (m, r) under the original action of R on M.)

[**Hint:** There are many straightforward axioms to check. Don't give too many details; one sentence per axiom should suffice (e.g., in part **(d)**, you can say "left distributivity for the left R^{op}-module M follows from right distributivity from the right R-module M", or even "the distributivity axioms for the new module boil down to the distributivity axioms for the old module"). In parts **(a)**, **(b)** and **(d)**, you only have to check the axioms that have to do with multiplication. In **(c)**, you can use basic properties of transposes of matrices without proof, as long as you say clearly which properties you are using. You will need to use the commutativity of S in one place.]

2.2 Remark

Parts **(b)** and **(c)** of this exercise gives some examples of rings R that are isomorphic to their opposite rings R^{op}. See `https://mathoverflow.net/questions/64370/` for examples of rings that are not.

2.3 Solution

We shall follow the PEMDAS convention for the order of operations, treating the new multiplication $\mathbin{\widetilde{\cdot}}$ as a multiplicative operation. Thus, the expression "$a \mathbin{\widetilde{\cdot}} b + c \mathbin{\widetilde{\cdot}} d$" will mean "$(a \mathbin{\widetilde{\cdot}} b) + (c \mathbin{\widetilde{\cdot}} d)$" rather than "$a \mathbin{\widetilde{\cdot}} (b + c) \mathbin{\widetilde{\cdot}} d$".

We are in the slightly confusing situation of having two different "multiplications" on one and the same set R: the original multiplication $\cdot$ of the ring R, and the new multiplication $\mathbin{\widetilde{\cdot}}$ of the ring R^{op} (although we still have not shown that R^{op} is actually a ring). Let us agree

that if $a, b \in R$, 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 $\widetilde{\cdot}$).

The original ring R satisfies all the ring axioms (since it is a ring). Thus, in particular, $(R, +, 0)$ is an abelian group, and $(R, \cdot, 1)$ is a monoid.

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

- **Additive axioms:** The triple $(R, +, 0_R)$ is an abelian group.
- **Multiplicative axioms:** The triple $(R, \widetilde{\cdot}, 1_R)$ is a monoid. This means, specifically, that the following hold:
  - **Associativity of multiplication:** We have $a \mathbin{\widetilde{\cdot}} (b \mathbin{\widetilde{\cdot}} c) = (a \mathbin{\widetilde{\cdot}} b) \mathbin{\widetilde{\cdot}} c$ for all $a, b, c \in R$. (Of course, we **cannot** use "ab" as an abbreviation for "$a \mathbin{\widetilde{\cdot}} b$", since "$ab$" already stands for the different product $a \cdot b$.)
  - **Neutrality of one:** We have $a \mathbin{\widetilde{\cdot}} 1_R = 1_R \mathbin{\widetilde{\cdot}} a = a$ for all $a \in R$.
- **Annihilation:** We have $a \mathbin{\widetilde{\cdot}} 0_R = 0_R \mathbin{\widetilde{\cdot}} a = 0_R$ for all $a \in R$.
- **Distributivity:** We have

$$a \mathbin{\widetilde{\cdot}} (b + c) = a \mathbin{\widetilde{\cdot}} b + a \mathbin{\widetilde{\cdot}} c \qquad \text{and} \qquad (a + b) \mathbin{\widetilde{\cdot}} c = a \mathbin{\widetilde{\cdot}} c + b \mathbin{\widetilde{\cdot}} c$$

  for all $a, b, c \in R$.

Some of these axioms are more obvious than others. In particular, the additive axioms clearly hold, since we already know that $(R, +, 0)$ is an abelian group. Let us now prove the "Associativity of multiplication" axiom, and leave the rest to the reader (since the arguments always follow the same pattern of rewriting the $\widetilde{\cdot}$-products in terms of $\cdot$-products and applying the ring axioms for the original ring R).

[*Proof of the "Associativity of multiplication" axiom:* Let $a, b, c \in R$. We must prove that $a \mathbin{\widetilde{\cdot}} (b \mathbin{\widetilde{\cdot}} c) = (a \mathbin{\widetilde{\cdot}} b) \mathbin{\widetilde{\cdot}} c$.

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

$$a \mathbin{\widetilde{\cdot}} (b \mathbin{\widetilde{\cdot}} c) = \underbrace{(b \mathbin{\widetilde{\cdot}} c)}_{=cb} a = (cb)\, a \tag{3}$$

and

$$(a \mathbin{\widetilde{\cdot}} b) \mathbin{\widetilde{\cdot}} c = c \underbrace{(a \mathbin{\widetilde{\cdot}} b)}_{=ba} = c\,(ba)\,. \tag{4}$$

But the original ring R 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 (3) and (4) are equal. Thus, their left hand sides are also equal. In other words, $a \mathbin{\widetilde{\cdot}} (b \mathbin{\widetilde{\cdot}} c) = (a \mathbin{\widetilde{\cdot}} b) \mathbin{\widetilde{\cdot}} c$. Thus, the "Associativity of multiplication" axiom is proven.]

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

(b) $\Longrightarrow$: Assume that $\mathrm{id} : R \to R$ is a ring isomorphism from R to R^{op}. We must prove that R is commutative.

We have assumed that id is a ring isomorphism from R to R^{op}. Thus, in particular, id is a ring morphism from R to R^{op}.

Recall that if U and V are two rings, and if f is a ring morphism from U to V, then

$$f(a \cdot b) = f(a) \cdot f(b) \qquad \text{for all } a, b \in U. \tag{5}$$

(Indeed, this is one of the four axioms in our definition of a ring morphism.) But keep in mind that the two "$\cdot$" signs in the equality (5) 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, (5) (applied to $U = R$, $V = R^{\mathrm{op}}$ and $f = \mathrm{id}$) yields

$$\mathrm{id}(a \cdot b) = \mathrm{id}(a) \mathbin{\widetilde{\cdot}} \mathrm{id}(b) \qquad \text{for all } a, b \in R \tag{6}$$

(since id is a ring morphism from R to R^{op}, and since the multiplication of the ring R is denoted by "$\cdot$" whereas the multiplication of the ring R^{op} is denoted by "$\mathbin{\widetilde{\cdot}}$").

Now, if $a, b \in R$, then

$$\begin{aligned} ab = a \cdot b = \mathrm{id}(a \cdot b) &= \underbrace{\mathrm{id}(a)}_{=a} \mathbin{\widetilde{\cdot}} \underbrace{\mathrm{id}(b)}_{=b} \qquad \text{(by (6))} \\ &= a \mathbin{\widetilde{\cdot}} b = ba \qquad \text{(by the definition of the operation } \mathbin{\widetilde{\cdot}}\text{)}. \end{aligned}$$

In other words, the ring R is commutative. This proves the "$\Longrightarrow$" direction of part **(b)**.

$\Longleftarrow$: Assume that R is commutative. We must prove that $\mathrm{id} : R \to R$ is a ring isomorphism from R to R^{op}.

If $a, b \in R$, then

$$\begin{aligned} a \mathbin{\widetilde{\cdot}} b &= ba \qquad \text{(by the definition of the operation } \mathbin{\widetilde{\cdot}}\text{)} \\ &= ab \qquad \text{(since the ring } R \text{ is commutative)} \\ &= a \cdot b. \end{aligned}$$

Thus, the binary operation $\mathbin{\widetilde{\cdot}}$ is identical with the binary operation $\cdot$.

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

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

(c) We shall use some basic properties of transposes of matrices (see, e.g., [Grinbe15, Exercise 6.5]):

Proposition 2.1. *Let S be a commutative ring. In this proposition, all matrices are over S.*

(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*

$$(PQ)^T = Q^T P^T.$$

(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 $\lambda \in S$, 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*

$$\left(P^T\right)^T = P.$$

Now, let $\mathbf{T}$ be the map

$$R \to R^{\mathrm{op}}, \qquad A \mapsto A^T.$$

We must prove that $\mathbf{T}$ is a ring isomorphism.

In Lecture 3, we have proven that any invertible ring morphism is a ring isomorphism. Hence, it suffices to prove that $\mathbf{T}$ is an invertible ring morphism.

Let us first prove that $\mathbf{T}$ is a ring morphism. In order to do so, we need to verify the following four claims:

Claim 1: We have $\mathbf{T}(a+b) = \mathbf{T}(a) + \mathbf{T}(b)$ for all $a, b \in R$.

Claim 2: We have $\mathbf{T}(0_R) = 0_{R^{\mathrm{op}}}$.

Claim 3: We have $\mathbf{T}(ab) = \mathbf{T}(a) \mathbin{\widetilde{\cdot}} \mathbf{T}(b)$ for all $a, b \in R$.

Claim 4: We have $\mathbf{T}(1_R) = 1_{R^{\mathrm{op}}}$.

(Note the "$\widetilde{\cdot}$" sign on the right hand side of Claim 3; this is because $\mathbf{T}(a)$ and $\mathbf{T}(b)$ are being considered as elements of R^{op}, and the multiplication of the ring R^{op} is $\widetilde{\cdot}$.)

Let us now prove these claims:

[*Proof of Claim 3:* Let $a, b \in R$. Then, $a \in R = S^{n \times n}$ and $b \in R = S^{n \times n}$. Hence, a and b are two $n \times n$-matrices over S. The definition of $\mathbf{T}$ yields $\mathbf{T}(ab) = (ab)^T$ and $\mathbf{T}(a) = a^T$ and $\mathbf{T}(b) = b^T$. The definition of the operation $\widetilde{\cdot}$ yields $\mathbf{T}(a) \mathbin{\widetilde{\cdot}} \mathbf{T}(b) = \underbrace{\mathbf{T}(b)}_{=b^T} \underbrace{\mathbf{T}(a)}_{=a^T} = b^T a^T$. But $\mathbf{T}(ab) = (ab)^T = b^T a^T$ (by Proposition 2.1 **(a)**, applied to $u = n$, $v = n$, $w = n$, $P = a$ and $Q = b$). Comparing these two equalities, we obtain $\mathbf{T}(ab) = \mathbf{T}(a) \mathbin{\widetilde{\cdot}} \mathbf{T}(b)$. This proves Claim 3.]

[*Proof of Claim 1:* Let $a, b \in R$. Then, $a \in R = S^{n \times n}$ and $b \in R = S^{n \times n}$. Hence, a and b are two $n \times n$-matrices over S. The definition of $\mathbf{T}$ yields $\mathbf{T}(a+b) = (a+b)^T$ and $\mathbf{T}(a) = a^T$ and $\mathbf{T}(b) = b^T$. But $\underbrace{\mathbf{T}(a)}_{=a^T} + \underbrace{\mathbf{T}(b)}_{=b^T} = a^T + b^T$. But $\mathbf{T}(a+b) = (a+b)^T = a^T + b^T$ (by Proposition 2.1 **(d)**, applied to $u = n$, $v = n$, $P = a$ and $Q = b$). Comparing these two equalities, we obtain $\mathbf{T}(a+b) = \mathbf{T}(a) + \mathbf{T}(b)$. This proves Claim 1.]

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

[*Proof of Claim 4:* We have $1_R = I_n$ (by the definition of the ring $R = S^{n \times n}$). Applying the map $\mathbf{T}$ to both sides of this equality, we obtain $\mathbf{T}(1_R) = \mathbf{T}(I_n) = (I_n)^T$ (by the

definition of $\mathbf{T}$). But Proposition 2.1 **(b)** (applied to $u = n$) yields $(I_n)^T = I_n$. Hence, $\mathbf{T}(1_R) = (I_n)^T = I_n$. But the definition of the ring R^{op} yields $1_{R^{\mathrm{op}}} = 1_R = I_n$. Comparing the latter two equalities, we obtain $\mathbf{T}(1_R) = 1_{R^{\mathrm{op}}}$. This proves Claim 4.]

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

Let us next prove that the map $\mathbf{T}$ 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 R and R^{op}, but can simply consider R and R^{op} as sets (because the invertibility of a map has nothing to do with any ring structures).

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

$$\begin{aligned}(\mathbf{T} \circ \mathbf{T})(P) &= \mathbf{T}\left(\underbrace{\mathbf{T}(P)}_{\substack{=P^T \\ \text{(by the definition of } \mathbf{T})}}\right) = \mathbf{T}\left(P^T\right) = \left(P^T\right)^T \qquad \text{(by the definition of } \mathbf{T}) \\ &= P \qquad \text{(by Proposition 2.1 } \mathbf{(e)} \text{ (applied to } u = n \text{ and } v = n)) \\ &= \mathrm{id}(P).\end{aligned}$$

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

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

(d) We have assumed that M is a right R-module. Thus, the module axioms hold. In other words, the following claims hold:

Claim 5: The triple $(M, +, 0)$ is an abelian group.

Claim 6: We have $m(r + s) = mr + ms$ for all $r, s \in R$ and $m \in M$.

Claim 7: We have $(m + n)r = mr + nr$ for all $r \in R$ and $m, n \in M$.

Claim 8: We have $m(rs) = (mr)s$ for all $r, s \in R$ and $m \in M$.

Claim 9: We have $m0_R = 0_M$ for every $m \in M$.

Claim 10: We have $0_M r = 0_M$ for every $r \in R$.

Claim 11: We have $m1 = m$ for every $m \in M$.

We must prove that M is a left R^{op}-module. In other words, we must prove that the module axioms for the left R^{op}-module hold:

Claim 12: The triple $(M, +, 0)$ is an abelian group.

Claim 13: We have $(r + s)m = rm + sm$ for all $r, s \in R^{\mathrm{op}}$ and $m \in M$.

Claim 14: We have $r(m + n) = rm + rn$ for all $r \in R^{\mathrm{op}}$ and $m, n \in M$.

Claim 15: We have $(r \mathbin{\widetilde{\cdot}} s)m = r(sm)$ for all $r, s \in R^{\mathrm{op}}$ and $m \in M$.

Claim 16: We have $0_R m = 0_M$ for every $m \in M$.

Claim 17: We have $r \cdot 0_M = 0_M$ for every $r \in R^{\mathrm{op}}$.

Claim 18: We have $1m = m$ for every $m \in M$.

Unsurprisingly, Claims 12–18 follow easily from Claims 5–11. For example, let us show how Claim 15 follows from Claim 8:

[*Proof of Claim 15:* Let $r, s \in R^{\mathrm{op}}$ and $m \in M$. Of course, from $r, s \in R^{\mathrm{op}}$, we obtain $r, s \in R$ (since $R^{\mathrm{op}} = R$ as sets).

The definition of the action of R^{op} on M yields $sm = ms$ and $r\,(sm) = \underbrace{(sm)}_{=ms} r = (ms)\, r$.

Also, the definition of the operation $\widetilde{\cdot}$ yields $r \mathbin{\widetilde{\cdot}} s = sr$. Hence,

$$\begin{aligned}(r \mathbin{\widetilde{\cdot}} s)\, m &= (sr)\, m = m\,(sr) && \text{(by the definition of the action of } R^{\mathrm{op}} \text{ on } M) \\ &= (ms)\, r && \text{(by Claim 8, applied to } s \text{ and } r \text{ instead of } r \text{ and } s)\,.\end{aligned}$$

Comparing this with $r\,(sm) = (ms)\, r$, we obtain $(r \mathbin{\widetilde{\cdot}} s)\, m = r\,(sm)$. This proves Claim 15.]

Thus, we have derived Claim 15 from Claim 8. Similarly, we can derive Claim 13 from Claim 6; Claim 14 from Claim 5; Claim 16 from Claim 9; Claim 17 from Claim 10; Claim 18 from Claim 11. Of course, Claim 12 is just a copy of Claim 5.

Now, all the Claims 12–18 are proved; thus, M is a left R^{op}-module.

---

3 Exercise 3

3.1 Problem

Let R be an integral domain. Let $a \in R$ and $b \in R$. Assume that a and b have an lcm $\ell \in R$. Prove that a and b have a gcd $g \in R$, which furthermore satisfies $g\ell = ab$.

[**Hint:** If u and v are two elements of an integral domain R, with $v \neq 0$, then you can use the notation $\dfrac{u}{v}$ (or u/v) for the element $w \in R$ satisfying $u = vw$. This element w does not always exist, but when it does, it is unique, so the notation is unambiguous. It is also easy to see that standard rules for fractions, such as $\dfrac{u}{v} + \dfrac{x}{y} = \dfrac{uy + vx}{vy}$ and $\dfrac{u}{v} \cdot \dfrac{x}{y} = \dfrac{ux}{vy}$, hold as long as the fractions $\dfrac{u}{v}$ and $\dfrac{x}{y}$ exist.]

3.2 Remark

The converse is not true: The existence of a gcd does not imply the existence of an lcm.

3.3 Solution sketch

We must prove that a and b have a gcd $g \in R$, which furthermore satisfies $g\ell = ab$. If $a = 0$ or $b = 0$, then this is easy[2]. Hence, for the rest of this proof, we WLOG assume that neither

[2]Indeed:

- If $a = 0$, then b is a gcd of a and b (indeed, we have $b \mid 0 = a$ and $b \mid b$, so that b is a common divisor of a and b, and furthermore it is clear that **every** common divisor of a and b is a divisor of b), and furthermore satisfies $b\ell = ab$ (indeed, ℓ is a multiple of a, so that $\ell = 0$ (since $a = 0$) and thus $\ell = 0 = a$, so that $b\ell = ba = ab$).
- If $b = 0$, then a is a gcd of a and b (for similar reasons), and furthermore satisfies $a\ell = ab$ (again for similar reasons).

$a = 0$ nor $b = 0$ holds. Thus, $a \neq 0$ and $b \neq 0$. Hence, $ab \neq 0$ (since R is an integral domain).

The element $\ell \in R$ is an lcm of a and b. In other words, ℓ is a common multiple of a and b with the property that **every** common multiple of a and b is a multiple of ℓ (by the definition of an lcm).

In particular, ℓ is a common multiple of a and b. In other words, $a \mid \ell$ and $b \mid \ell$. On the other hand, ab is clearly a common multiple of a and b, and thus is a multiple of ℓ (since **every** common multiple of a and b is a multiple of ℓ). In other words, $\ell \mid ab$. Hence, there exists some $m \in R$ such that $ab = \ell m$. Consider this m.

Now, we claim that $m \mid a$. Indeed, there exists some $y \in R$ such that $\ell = by$ (since $b \mid \ell$). Consider this y. Then, $ab = \underbrace{\ell}_{=by} m = bym$, so that $b(a - ym) = \underbrace{ba}_{=ab=bym} - bym = bym - bym = 0$. Since R is an integral domain, we thus conclude that $b = 0$ or $a - ym = 0$. Hence, $a - ym = 0$ (since $b \neq 0$). Therefore, $a = ym$, so that $m \mid a$.

A similar argument shows that $m \mid b$. From $m \mid a$ and $m \mid b$, we conclude that m is a common divisor of a and b.

Next, we shall show that **every** common divisor of a and b is a divisor of m. Indeed, let d be a common divisor of a and b. Then, $d \mid a$ and $d \mid b$.

From $d \mid a \mid ab$, we see that there exists some $z \in R$ such that $ab = dz$. Consider this z.

We shall show that $b \mid z$. Indeed, there exists some $x \in R$ such that $a = dx$ (since $d \mid a$). Consider this x. From $ab = dz$, we obtain $dz = \underbrace{a}_{=dx} b = dxb$ and thus $\underbrace{a}_{=dx} z = dxz = x \underbrace{dz}_{=dxb} = xdxb = \underbrace{dx}_{=a} xb = axb$. Hence, $a(z - xb) = \underbrace{az}_{=axb} - axb = axb - axb = 0$. Since R is an integral domain, we thus conclude that $a = 0$ or $z - xb = 0$. Hence, $z - xb = 0$ (since $a \neq 0$). Therefore, $z = xb$, so that $b \mid z$.

A similar argument shows that $a \mid z$. From $a \mid z$ and $b \mid z$, we conclude that z is a common multiple of a and b. Hence, z is a multiple of ℓ (since **every** common multiple of a and b is a multiple of ℓ). In other words, there exists some $w \in R$ such that $z = \ell w$. Consider this w.

Comparing $ab = \ell m$ with $ab = dz$, we find $\ell m = d \underbrace{z}_{=\ell w} = d\ell w$. Hence, $\underbrace{ab}_{=\ell m} m = \underbrace{\ell m}_{=d\ell w} m = d\ell wm = \underbrace{\ell m}_{=ab} dw = abdw$, so that

$$ab(m - dw) = \underbrace{abm}_{=abdw} - abdw = abdw - abdw = 0.$$

Since R is an integral domain, we thus conclude that $ab = 0$ or $m - dw = 0$. Hence, $m - dw = 0$ (since $ab \neq 0$). Therefore, $m = dw$, so that $d \mid m$. In other words, d is a divisor of m.

Now, forget that we fixed d. We thus have shown that every common divisor d of a and b is a divisor of m. Thus, we now know that m is a common divisor of a and b with the property that **every** common divisor of a and b is a divisor of m. In other words, m is a gcd of a and b (by the definition of a gcd). Moreover, this gcd m satisfies $m\ell = ab$ (since $m\ell = \ell m = ab$). Hence, a and b have a gcd $g \in R$, which furthermore satisfies $g\ell = ab$ (namely, $g = m$). This solves the exercise.

3.4 Remark

The above solution would have become more transparent if we had used the fraction notation suggested in the hint. Indeed, using this notation, our definitions of m, y, z, x, w could be

rewritten as

$$m = \frac{ab}{\ell}, \qquad y = \frac{\ell}{b}, \qquad z = \frac{ab}{d}, \qquad x = \frac{a}{d}, \qquad w = \frac{z}{\ell}.$$

---

4 Exercise 4

4.1 Problem

Let p be a prime number.

(a) Prove that if a and b are two integers such that $a^2 \equiv b^2 \mod p^2$, then $a \equiv b \mod p^2$ or $a \equiv -b \mod p^2$ or $a \equiv b \equiv 0 \mod p$.

(b) Compute the number of squares in the ring $\mathbb{Z}/p^2$.

4.2 Remark

This is one more step on our quest to count the squares in $\mathbb{Z}/n$ for an arbitrary positive integer n.

4.3 Solution sketch

This is rather similar to Exercise 10 on homework set #1, except that now the field F has been replaced by the ring $\mathbb{Z}/p^2$ (which is not a field, but behaves similarly in some ways).

(a) Let a and b be two integers such that $a^2 \equiv b^2 \bmod p^2$. We must prove that $a \equiv b \mod p^2$ or $a \equiv -b \mod p^2$ or $a \equiv b \equiv 0 \mod p$.

We assume the contrary. Thus, we have neither $a \equiv b \mod p^2$ or $a \equiv -b \mod p^2$ or $a \equiv b \equiv 0 \mod p$. We are trying to find a contradiction.

We have $a^2 \equiv b^2 \bmod p^2$, so that $p^2 \mid a^2 - b^2$ and therefore $p \mid p^2 \mid a^2 - b^2$.

We are in one of the following two cases:

Case 1: We have $p = 2$.

Case 2: We have $p \neq 2$.

Let us first consider Case 1. In this case, we have $p = 2$. Hence, $2 = p \mid a^2 - b^2$. In other words, $a^2 \equiv b^2 \bmod 2$. Now,

$$\begin{aligned}(a-b)^2 &= \underbrace{a^2}_{\equiv b^2 \bmod 2} - \underbrace{2}_{\equiv 0 \bmod 2} ab + b^2 \equiv b^2 - 0ab + b^2 = \underbrace{2}_{\equiv 0 \bmod 2} b^2 \\ &\equiv 0b^2 = 0 \bmod 2.\end{aligned}$$

In other words, $(a-b)^2$ is even. However, if the integer $a-b$ was odd, then its square $(a-b)^2$ would also be odd (since the square of an odd integer must be odd); this would contradict the fact that $(a-b)^2$ is even. Hence, the integer $a-b$ cannot be odd. Thus, $a-b$ must be even. In other words,

$$a - b = 2u \qquad \text{for some } u \in \mathbb{Z}.$$

Consider this u.

We have $p = 2$ and thus $p^2 = 2^2 = 4$.

We are in one of the following three subcases:

Subcase 1.1: The integer u is even.

Subcase 1.2: The integer $u + b$ is even.

Subcase 1.3: None of the two integers u and $u + b$ is even.

Let us first consider Subcase 1.1. In this subcase, the integer u is even. Hence, $u = 2v$ for some $v \in \mathbb{Z}$. Consider this v. Now, $a - b = 2\underbrace{u}_{=2v} = 2 \cdot 2v = 4v \equiv 0 \bmod 4$, so that $a \equiv b \bmod 4$. In other words, $a \equiv b \bmod p^2$ (since $p^2 = 4$). This contradicts the fact that we don't have $a \equiv b \bmod p^2$. Hence, we have found a contradiction in Subcase 1.1.

Let us next consider Subcase 1.2. In this subcase, the integer $u + b$ is even. Hence, $u + b = 2w$ for some $w \in \mathbb{Z}$. Consider this w. Now,

$$a - (-b) = a + b = \underbrace{(a - b)}_{=2u} + 2b = 2u + 2b = 2\underbrace{(u + b)}_{=w} = 2 \cdot 2w = 4w \equiv 0 \bmod 4,$$

so that $a \equiv -b \bmod 4$. In other words, $a \equiv -b \bmod p^2$ (since $p^2 = 4$). This contradicts the fact that we don't have $a \equiv -b \bmod p^2$. Hence, we have found a contradiction in Subcase 1.2.

Let us next consider Subcase 1.3. In this subcase, none of the two integers u and $u + b$ is even. Hence, both of these integers are odd. Thus, their sum $u + (u + b)$ must be even (since a sum of two odd integers is always even). In other words, $u + (u + b) = 2x$ for some $x \in \mathbb{Z}$. Consider this x. Now, $2u + b = u + (u + b) = 2x$, so that $b = 2x - 2u = 2(x - u) \equiv 0 \bmod 2$. Also, from $a - b = 2u \equiv 0 \bmod 2$, we obtain $a \equiv b \bmod 2$. Thus, $a \equiv b \equiv 0 \bmod 2$. In other words, $a \equiv b \equiv 0 \bmod p$ (since $p = 2$). This contradicts the fact that we don't have $a \equiv b \equiv 0 \bmod p$. Hence, we have found a contradiction in Subcase 1.3.

We have now found a contradiction in each of the three Subcases 1.1, 1.2 and 1.3. Hence, we always obtain a contradiction in Case 1.

Let us now consider Case 2. In this case, we have $p \neq 2$. Hence, $p > 2$ (since p is a prime).

Recall that $p \mid a^2 - b^2 = (a - b)(a + b)$. Since p is a prime, this entails that we must have $p \mid a - b$ or $p \mid a + b$ (since a prime that divides a product of two integers must always divide one of the two factors). Thus, we are in one of the following three subcases:

Subcase 2.1: We have $p \mid a - b$ and $p \mid a + b$.

Subcase 2.2: We have $p \mid a - b$ but not $p \mid a + b$.

Subcase 2.3: We have $p \mid a + b$ but not $p \mid a - b$.

Let us first consider Subcase 2.1. In this case, we have $p \mid a - b$ and $p \mid a + b$. Now,

$$2a = \underbrace{(a - b)}_{\substack{\equiv 0 \bmod p \\ (\text{since } p \mid a-b)}} + \underbrace{(a + b)}_{\substack{\equiv 0 \bmod p \\ (\text{since } p \mid a+b)}} \equiv 0 + 0 = 0 \bmod p,$$

so that $p \mid 2a$. But p is a prime; hence, if p divides a product of two integers, then p must divide one of its factors. Thus, from $p \mid 2a$, we obtain that $p \mid 2$ or $p \mid a$. Since $p \mid 2$ is impossible (because $p \mid 2$ would imply $p \leq 2$, contradicting $p > 2$), we thus must have $p \mid a$. In other words, $a \equiv 0 \bmod p$. Also, from $p \mid a - b$, we obtain $a \equiv b \bmod p$, so that $b \equiv a \equiv 0 \bmod p$. Combining this with $a \equiv 0 \bmod p$, we find $a \equiv b \equiv 0 \bmod p$. This contradicts the fact that we don't have $a \equiv b \equiv 0 \bmod p$. Hence, we have found a contradiction in Subcase 2.1.

Let us next consider Subcase 2.2. In this case, we have $p \mid a - b$ but not $p \mid a + b$.

However, p is a prime. Thus, each integer k is either divisible by p or coprime to p. Applying this to $k = a + b$, we conclude that $a + b$ is either divisible by p or coprime to p.

Since $a+b$ is not divisible by p (because we don't have $p \mid a+b$), we thus conclude that $a+b$ is coprime to p. In other words, p is coprime to $a+b$. Hence, p^2 is coprime to $a+b$ (since powers of coprime integers are still coprime).

Recall a classical fact from elementary number theory: If three integers u, v and w satisfy $u \mid vw$, and if u is coprime to v, then $u \mid w$. We can apply this to $u = p^2$, $v = a+b$ and $w = a-b$ (since $p^2 \mid a^2 - b^2 = (a+b)(a-b)$, and since p^2 is coprime to $a+b$). Thus we obtain $p^2 \mid a-b$. In other words, $a \equiv b \bmod p^2$. This contradicts the fact that we don't have $a \equiv b \bmod p^2$. Hence, we have found a contradiction in Subcase 2.2.

Let us next consider Subcase 2.3. In this case, we have $p \mid a+b$ but not $p \mid a-b$.

However, p is a prime. Thus, each integer k is either divisible by p or coprime to p. Applying this to $k = a-b$, we conclude that $a-b$ is either divisible by p or coprime to p. Since $a-b$ is not divisible by p (because we don't have $p \mid a-b$), we thus conclude that $a-b$ is coprime to p. In other words, p is coprime to $a-b$. Hence, p^2 is coprime to $a-b$ (since powers of coprime integers are still coprime).

Recall a classical fact from elementary number theory: If three integers u, v and w satisfy $u \mid vw$, and if u is coprime to v, then $u \mid w$. We can apply this to $u = p^2$, $v = a-b$ and $w = a+b$ (since $p^2 \mid a^2 - b^2 = (a-b)(a+b)$, and since p^2 is coprime to $a-b$). Thus we obtain $p^2 \mid a+b = a-(-b)$. In other words, $a \equiv -b \bmod p^2$. This contradicts the fact that we don't have $a \equiv -b \bmod p^2$. Hence, we have found a contradiction in Subcase 2.3.

We have now found a contradiction in each of the three Subcases 2.1, 2.2 and 2.3. Hence, we always obtain a contradiction in Case 2.

Now we know that we obtain a contradiction in both Cases 1 and 2. This shows that our assumption was false. Part **(a)** of the exercise is thus solved.

(b) Let $F = \mathbb{Z}/p^2$. Thus, F is a commutative ring of size $|F| = |\mathbb{Z}/p^2| = p^2$.

Note that F is not a field; we have only called it F to stress the analogy with the F in Exercise 10 on homework set #1.

We have the following:

Claim 1: Let $d \in F$. Then:

(i) If d is not a unit of F, then $d^2 = 0$.

(ii) If d is a unit of F, then d^2 is a unit of F.

Proof of Claim 1. **(i)** Assume that d is not a unit of F. We have $d \in F = \mathbb{Z}/p^2$; thus, there exists some $a \in \mathbb{Z}$ such that $d = \overline{a}$. Consider this a. Recall that d is not a unit of F. In other words, $\overline{a}$ is not a unit of $\mathbb{Z}/p^2$ (since $d = \overline{a}$ and $F = \mathbb{Z}/p^2$).

Recall the following fact (proven in Lecture 2): The residue class $\overline{a} \in \mathbb{Z}/n$ (for some integer n) is a unit of $\mathbb{Z}/n$ if and only if a is coprime to n. Applying this to $n = p^2$, we conclude that $\overline{a}$ is a unit of $\mathbb{Z}/p^2$ if and only if a is coprime to p^2. Hence, a is not coprime to p^2 (since $\overline{a}$ is not a unit of $\mathbb{Z}/p^2$).

However, p is a prime. Thus, each integer k is either divisible by p or coprime to p. Applying this to $k = a$, we conclude that a is either divisible by p or coprime to p. Thus, if a was not divisible by p, then a would be coprime to p and therefore also coprime to p^2 (since powers of coprime integers are still coprime); but this would contradict the fact that a is not coprime to p^2. Hence, a must be divisible by p. Thus, a^2 is divisible by p^2. In other words, $a^2 \equiv 0 \bmod p^2$. In other words, $\overline{a^2} = 0$ in $\mathbb{Z}/p^2$. Now, from $d = \overline{a}$, we obtain $d^2 = \overline{a}^2 = \overline{a^2} = 0$. This proves Claim 1 **(i)**.

(ii) Assume that d is a unit of F. Recall that the units of F form a group under multiplication. Hence, any product of two units of F is a unit of F. Thus, the product dd

is a unit of F (since d and d are units of F). In other words, d^2 is a unit of F. This proves Claim 1 **(ii)**. $\square$

Claim 2: Let x, y be two units of F such that $x^2 = y^2$. Then, $x = y$ or $x = -y$.

Proof of Claim 2. We have $x \in F = \mathbb{Z}/p^2$. Thus, there exists some $a \in \mathbb{Z}$ such that $x = \overline{a}$. Similarly, there exists some $b \in \mathbb{Z}$ such that $y = \overline{b}$. Consider these a and b. We have assumed that $x^2 = y^2$. In view of $x = \overline{a}$ and $y = \overline{b}$, this rewrites as $\overline{a}^2 = \overline{b}^2$. Thus, $\overline{a^2} = \overline{a}^2 = \overline{b}^2 = \overline{b^2}$. In other words, $a^2 \equiv b^2 \bmod p^2$. According to part **(a)** of this exercise, we can thus conclude that $a \equiv b \bmod p^2$ or $a \equiv -b \bmod p^2$ or $a \equiv b \equiv 0 \bmod p$. Hence, we are in one of the following three cases:

Case 1: We have $a \equiv b \bmod p^2$.

Case 2: We have $a \equiv -b \bmod p^2$.

Case 3: We have $a \equiv b \equiv 0 \bmod p$.

Let us first consider Case 1. In this case, we have $a \equiv b \bmod p^2$. In other words, $\overline{a} = \overline{b}$ in $\mathbb{Z}/p^2$. Hence, $x = \overline{a} = \overline{b} = y$. Thus, we have $x = y$ or $x = -y$ (namely, we have $x = y$). Claim 2 is thus proven in Case 1.

Let us next consider Case 2. In this case, we have $a \equiv -b \bmod p^2$. In other words, $\overline{a} = \overline{-b}$ in $\mathbb{Z}/p^2$. Hence, $x = \overline{a} = \overline{-b} = -\underbrace{\overline{b}}_{=y} = -y$. Thus, we have $x = y$ or $x = -y$ (namely, we have $x = -y$). Claim 2 is thus proven in Case 2.

Finally, let us consider Case 3. In this case, we have $a \equiv b \equiv 0 \bmod p$. Hence, $a \equiv 0 \bmod p$, so that a is divisible by p. Thus, a^2 is divisible by p^2. In other words, $a^2 \equiv 0 \bmod p^2$. In other words, $\overline{a^2} = 0$ in $\mathbb{Z}/p^2$. But $x = \overline{a}$ and thus $x^2 = \overline{a}^2 = \overline{a^2} = 0$. However, x is a unit of F; thus, we can divide both sides of this equality $x^2 = 0$ by x. We thus obtain $x = 0$. Similarly, we find $y = 0$. Thus, $x = 0 = y$. Hence, we have $x = y$ or $x = -y$ (namely, we have $x = y$). Claim 2 is thus proven in Case 3.

We have now proven Claim 2 in each of the three Cases 1, 2 and 3. Hence, Claim 2 is proved. $\square$

Claim 3: Let $c \in F$. Then:

(i) If c is a nonzero square, then

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

(ii) If c is not a square, then

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

(iii) If $c = 0$, then

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

Proof of Claim 3. **(i)** Assume that c is a nonzero square. Thus, there exists a $g \in F$ such that $c = g^2$ (since c is a square). Consider this g. Using the ring axioms, we can easily see that $(-g)^2 = g^2$ (just as this identity is proved for numbers). Hence, $c = (-g)^2$ (since $c = g^2$). Also, from $c = g^2$, we obtain $g^2 = c \neq 0$ (since c is nonzero).

If g was not a unit of F, then we would have $g^2 = 0$ (by Claim 1 **(i)**, applied to $d = g$); but this would contradict $g^2 \neq 0$. Hence, g must be a unit of F.

Since $p > 1$, we have $p^2 > p \geq 2$ and thus $p^2 \nmid 2$. In other words, $2 \not\equiv 0 \bmod p^2$.

We have $F = \mathbb{Z}/p^2$ and thus $1_F = \overline{1}$, so that $1_F + 1_F = \overline{1} + \overline{1} = \overline{1+1} = \overline{2} \neq \overline{0}$ (since $2 \not\equiv 0 \bmod p^2$). In other words, $1_F \neq -1_F$.

Now, if we had $g = -g$, then we could divide both sides of this equality by g (since g is a unit of F), and thus obtain $1_F = -1_F$; but this would contradict $1_F \neq -1_F$. Hence, we cannot have $g = -g$. Therefore, $g \neq -g$, so that $|\{g, -g\}| = 2$.

But both g and $-g$ belong to the set $\{d \in F \mid c = d^2\}$ (since $g, -g \in F$ and $c = g^2$ and $c = (-g)^2$). Hence,

$$\{g, -g\} \subseteq \left\{d \in F \mid c = d^2\right\}. \tag{7}$$

On the other hand, let us prove that $\{d \in F \mid c = d^2\} \subseteq \{g, -g\}$. Indeed, let $a \in \{d \in F \mid c = d^2\}$. Thus, a is an element of F and satisfies $c = a^2$. Hence, $a^2 = c \neq 0$. If a was not a unit of F, then we would have $a^2 = 0$ (by Claim 1 **(i)**, applied to $d = a$); but this would contradict $a^2 \neq 0$. Hence, a must be a unit of F. Now, we know that a and g are units of F and satisfy $a^2 = c = g^2$. Hence, Claim 2 (applied to $x = a$ and $y = g$) 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 $a \in \{d \in F \mid c = d^2\}$. In other words, $\{d \in F \mid c = d^2\} \subseteq \{g, -g\}$. Combining this with (7), we obtain

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

Hence,

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

This proves Claim 3 **(i)**.

(ii) Assume that c is not a square. Then, there exists no $\alpha \in F$ such that $c = \alpha^2$ (by the definition of a square). In other words, there exists no $d \in F$ such that $c = d^2$ (here, we have renamed the index α as d). In other words, $\{d \in F \mid c = d^2\} = \varnothing$. Hence, $|\{d \in F \mid c = d^2\}| = |\varnothing| = 0$. This proves Claim 3 **(ii)**.

(iii) Assume that $c = 0$.

Note that the p integers $0p, 1p, \ldots, (p-1)\,p$ are distinct and all belong to $\{0, 1, \ldots, p^2 - 1\}$; hence, their residue classes $\overline{0p}, \overline{1p}, \ldots, \overline{(p-1)\,p}$ modulo p^2 are distinct. In other words, $\left|\left\{\overline{0p}, \overline{1p}, \ldots, \overline{(p-1)\,p}\right\}\right| = p$.

Let P be the subset $\left\{\overline{0p}, \overline{1p}, \ldots, \overline{(p-1)\,p}\right\}$ of F. Thus, $P = \left\{\overline{0p}, \overline{1p}, \ldots, \overline{(p-1)\,p}\right\}$, so that

$$|P| = \left|\left\{\overline{0p}, \overline{1p}, \ldots, \overline{(p-1)\,p}\right\}\right| = p.$$

Now, it is easy to see that each $d \in P$ satisfies $c = d^2$ [3]. In other words, $P \subseteq \{d \in F \mid c = d^2\}$.

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

Indeed, let $a \in \{d \in F \mid c = d^2\}$. Thus, $a \in F$ and $c = a^2$. Hence, $a^2 = c = 0$.

We have $a \in F = \mathbb{Z}/p^2$. In other words, $a = \overline{u}$ for some $u \in \mathbb{Z}$. Consider this u. From $a = \overline{u}$, we obtain $a^2 = \overline{u}^2 = \overline{u^2}$, so that $\overline{u^2} = a^2 = 0 = \overline{0}$. In other words, $u^2 \equiv 0 \bmod p^2$. Hence, $p^2 \mid u^2$. Thus, $\gcd(p^2, u^2) = p^2 > 1$ (since $p > 1$).

However, p is a prime. Thus, each integer k is either divisible by p or coprime to p. Applying this to $k = u$, we conclude that u is either divisible by p or coprime to p. Thus, if

[3] *Proof.* Let $d \in P$. We must show that $c = d^2$.

We have $d \in P = \left\{\overline{0p}, \overline{1p}, \ldots, \overline{(p-1)\,p}\right\}$. In other words, $d = \overline{kp}$ for some $k \in \{0, 1, \ldots, p-1\}$. Consider this k. Now, from $d = \overline{kp}$, we obtain

$$d^2 = \overline{kp}^2 = \overline{(kp)^2} = \overline{0} \qquad \left(\text{since } (kp)^2 = k^2p^2 \equiv 0 \bmod p^2\right)$$
$$= 0.$$

Comparing this with $c = 0$, we obtain $c = d^2$, qed.

u was not divisible by p, then u would be coprime to p, and therefore u^2 would be coprime to p^2 (since powers of coprime integers are still coprime); but this would contradict the fact that $\gcd\left(p^2, u^2\right) > 1$. Hence, u must be divisible by p. In other words, $u = pv$ for some $v \in \mathbb{Z}$. Consider this v.

Let q and r be the quotient and the remainder obtained when dividing v by p. Thus, $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, p-1\}$ and $v = qp + r$. Now,

$$u = p \underbrace{v}_{=qp+r} = p\left(qp + r\right) = \underbrace{qp^2}_{\equiv 0 \bmod p^2} + rp \equiv rp \bmod p^2,$$

so that

$$\begin{aligned} \overline{u} = \overline{rp} &\in \left\{\overline{0p}, \overline{1p}, \ldots, \overline{(p-1)\,p}\right\} \qquad \left(\text{since } r \in \{0, 1, \ldots, p-1\}\right) \\ &= P. \end{aligned}$$

Hence, $a = \overline{u} \in P$.

Now, forget that we fixed a. We thus have shown that $a \in P$ for each $a \in \{d \in F \mid c = d^2\}$. In other words, $\{d \in F \mid c = d^2\} \subseteq P$. Combining this with $P \subseteq \{d \in F \mid c = d^2\}$, we obtain $\{d \in F \mid c = d^2\} = P$. Hence, $|\{d \in F \mid c = d^2\}| = |P| = p$. This proves Claim 3 **(iii)**. □

Now, let us count all pairs $(c, d) \in F \times F$ 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 $c \in F$). Thus, we find

$$\begin{aligned} &\left(\text{the number of all } (c,d) \in F \times F \text{ such that } c = d^2\right) \\ &= \sum_{c \in F} \underbrace{\left(\text{the number of all } d \in F \text{ such that } c = d^2\right)}_{=\left|\{d \in F \mid c = d^2\}\right|} \\ &= \sum_{c \in F} \left|\left\{d \in F \mid c = d^2\right\}\right| \\ &= \sum_{\substack{c \in F; \\ c = 0}} \underbrace{\left|\left\{d \in F \mid c = d^2\right\}\right|}_{\substack{=p \\ \text{(by Claim 3 (iii))}}} + \sum_{\substack{c \in F; \\ c \text{ is a nonzero square}}} \underbrace{\left|\left\{d \in F \mid c = d^2\right\}\right|}_{\substack{=2 \\ \text{(by Claim 3 (i))}}} \\ &\quad + \sum_{\substack{c \in F; \\ c \text{ is not a square}}} \underbrace{\left|\left\{d \in F \mid c = d^2\right\}\right|}_{\substack{=0 \\ \text{(by Claim 3 (ii))}}} \\ &\qquad \left(\begin{array}{c} \text{because each } c \in F \text{ satisfies exactly one of the three statements} \\ \text{“}c = 0\text{”, “}c \text{ is a nonzero square” and “}c \text{ is not a square”} \end{array}\right) \\ &= \underbrace{\sum_{\substack{c \in F; \\ c = 0}} p}_{\substack{=p \\ \text{(since this sum has} \\ \text{exactly one addend)}}} + \underbrace{\sum_{\substack{c \in F; \\ c \text{ is a nonzero square}}} 2}_{=2 \cdot (\text{the number of nonzero squares in } F)} + \underbrace{\sum_{\substack{c \in F; \\ c \text{ is not a square}}} 0}_{=0} \\ &= p + 2 \cdot (\text{the number of nonzero squares in } F) + 0 \\ &= p + 2 \cdot (\text{the number of nonzero squares in } F). \end{aligned}$$

- 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 $d \in F$). Thus, we find

$$\begin{aligned}
&\left(\text{the number of all } (c,d) \in F \times F \text{ such that } c = d^2\right) \\
&= \sum_{d \in F} \underbrace{\left(\text{the number of all } c \in F \text{ such that } c = d^2\right)}_{=1} \\
&\qquad \left(\text{since there is exactly one } c \in F \text{ such that } c = d^2 \text{ (namely, } c = d^2\text{)}\right) \\
&= \sum_{d \in F} 1 = |F| \cdot 1 = |F| .
\end{aligned}$$

Comparing these two equalities, we obtain

$$|F| = p + 2 \cdot (\text{the number of nonzero squares in } F) .$$

Solving this for (the number of nonzero squares in F), we find

$$(\text{the number of nonzero squares in } F) = \frac{|F| - p}{2} = \frac{p^2 - p}{2}$$

(since $|F| = p^2$).

Now, there are two kinds of squares in F: namely, the nonzero squares (of which there are exactly $\dfrac{p^2 - p}{2}$ 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 F is $\dfrac{p^2 - p}{2} + 1$. In other words, the total number of squares in $\mathbb{Z}/p^2$ is $\dfrac{p^2 - p}{2} + 1$ (since $F = \mathbb{Z}/p^2$). This solves part **(b)** of the exercise.

---

5 Exercise 5

5.1 Problem

Let p be a prime number.

(a) Prove that the only units of the ring $\mathbb{Z}/p$ that are their own inverses (i.e., the only $m \in (\mathbb{Z}/p)^\times$ that satisfy $m^{-1} = m$) are $\overline{1}$ and $\overline{-1}$.

(b) Assume that p is odd. Let $u = \dfrac{p-1}{2} \in \mathbb{N}$. Prove that $u!^2 \equiv -(-1)^u \mod p$.

[**Hint:** The two parts of the exercise are unrelated, other than both being lemmas in our Lecture 7. For part **(b)**, recall Wilson's theorem.]

5.2 Remark

Part **(b)** of this exercise easily yields that $u!^2 \equiv -1 \mod p$ if $p \equiv 1 \mod 4$ (since $p \equiv 1 \mod 4$ entails that u is even). This is one of the facts we used in Lecture 7.]

5.3 Solution

(a) We have $\overline{1} \cdot \overline{1} = \overline{1 \cdot 1} = \overline{1}$ and $\overline{-1} \cdot \overline{-1} = \overline{(-1) \cdot (-1)} = \overline{1}$. Thus, the elements $\overline{1}$ and $\overline{-1}$ of $\mathbb{Z}/p$ are inverse to themselves. Hence, these elements $\overline{1}$ and $\overline{-1}$ have inverses, i.e., are units of $\mathbb{Z}/p$. Since they are inverse to themselves, we thus conclude that they are units of the ring $\mathbb{Z}/p$ that are their own inverses.

It remains to prove that they are the **only** such units. In other words, it remains to prove that if a is a unit of $\mathbb{Z}/p$ that is its own inverse, then a equals $\overline{1}$ or $\overline{-1}$.

So let a be a unit of $\mathbb{Z}/p$ that is its own inverse. We must prove that a equals $\overline{1}$ or $\overline{-1}$.

Indeed, $\mathbb{Z}/p$ is a field (since p is prime), hence an integral domain. But a is its own inverse; in other words, $aa = \overline{1}$ (since $\overline{1}$ is the unity of the ring $\mathbb{Z}/p$). Now, $\left(a - \overline{1}\right)\left(a + \overline{1}\right) = a^2 - \overline{1}^2 = 0$ (since $a^2 = aa = \overline{1} = \overline{1}^2$). Since $\mathbb{Z}/p$ is an integral domain, we thus conclude that we have $a - \overline{1} = 0$ or $a + \overline{1} = 0$. In other words, we have $a = \overline{1}$ or $a = -\overline{1}$. In other words, a equals $\overline{1}$ or $-\overline{1}$. In other words, a equals $\overline{1}$ or $\overline{-1}$ (since $-\overline{1} = \overline{-1}$). But this is precisely what we wanted to prove. Thus, the solution to part **(a)** is complete.

(b) We have $p - 1 = 2u$ (since $u = \dfrac{p-1}{2}$), so that $p - 2u = 1$. Also, $p - (u+1) = \underbrace{p-1}_{=2u} - u = 2u - u = u$.

Wilson's theorem yields $(p-1)! \equiv -1 \bmod p$. Hence,

$$\begin{aligned} -1 &\equiv (p-1)! \\ &= 1 \cdot 2 \cdot \cdots \cdot (p-1) \\ &= 1 \cdot 2 \cdot \cdots \cdot (2u) \qquad \text{(since } p-1 = 2u\text{)} \\ &= (1 \cdot 2 \cdot \cdots \cdot u) \cdot ((u+1) \cdot (u+2) \cdot \cdots \cdot (2u)) \bmod p. \end{aligned} \tag{8}$$

However,

$$\begin{aligned} &(u+1) \cdot (u+2) \cdot \cdots \cdot (2u) \\ &= \prod_{k=u+1}^{2u} k = \prod_{j=p-2u}^{p-(u+1)} \underbrace{(p-j)}_{\equiv -j \bmod p} \\ &\qquad \text{(here, we have substituted } p-j \text{ for } k \text{ in the product)} \\ &\equiv \prod_{j=p-2u}^{p-(u+1)} (-j) = \prod_{j=1}^{u} (-j) \qquad \text{(since } p-2u = 1 \text{ and } p-(u+1) = u\text{)} \\ &= (-1)^u \underbrace{\prod_{j=1}^{u} j}_{=1 \cdot 2 \cdot \cdots \cdot u = u!} = (-1)^u u! \bmod p. \end{aligned}$$

Hence, (8) becomes

$$-1 \equiv \underbrace{(1 \cdot 2 \cdot \cdots \cdot u)}_{=u!} \cdot \underbrace{((u+1) \cdot (u+2) \cdot \cdots \cdot (2u))}_{\equiv (-1)^u u! \bmod p} \equiv u! \cdot (-1)^u u! = (-1)^u (u!)^2 \bmod p.$$

Multiplying both sides of this congruence by $(-1)^u$, we obtain

$$-(-1)^u \equiv \underbrace{(-1)^u (-1)^u}_{=(-1)^{2u}=1} (u!)^2 = (u!)^2 \bmod p.$$

Thus, $(u!)^2 \equiv -(-1)^u \bmod p$. This solves part **(b)** of the exercise.

---

6 Exercise 6

6.1 Problem

Recall the ring $\mathbb{Z}[i]$ of Gaussian integers. Let $N : \mathbb{Z}[i] \to \mathbb{N}$ be the map that sends each Gaussian integer $z = a + bi \in \mathbb{Z}[i]$ (with $a, b \in \mathbb{Z}$) to $a^2 + b^2 = |z|^2$. (This is the Euclidean norm on $\mathbb{Z}[i]$ that we have already used several times.)

(a) Prove that if z and w are two Gaussian integers satisfying $z \mid w$ in $\mathbb{Z}[i]$, then $N(z) \mid N(w)$ in $\mathbb{Z}$.

(b) Let $z = a + bi \in \mathbb{Z}[i]$ with $a, b \in \mathbb{Z}$. Assume that $z \neq 0$. Let $n = \lfloor |z| \rfloor = \left\lfloor \sqrt{a^2 + b^2} \right\rfloor$. Prove that every divisor of z in $\mathbb{Z}[i]$ has the form $c+di$ with $c, d \in \{-n, -n+1, \ldots, n\}$.

(c) Without recourse to the general theory of PIDs and UFDs, prove that every nonzero element of $\mathbb{Z}[i]$ has an irreducible factorization.

(d) Let $z \in \mathbb{Z}[i]$. Prove that we have the following logical equivalence:

$$(z \text{ is a unit of } \mathbb{Z}[i]) \iff (N(z) = 1) \iff (z \in \{1, i, -1, -i\}).$$

6.2 Remark

Combining parts **(b)** and **(c)** of this exercise yields a (slow) algorithm for finding an irreducible factorization of a nonzero Gaussian integer. (Indeed, part **(b)** shows that we can list all divisors of a nonzero Gaussian integer in finite time. This allows checking whether a Gaussian integer is prime, and otherwise finding a prime divisor.)

6.3 Solution sketch

Recall that

$$N(\alpha\beta) = N(\alpha) N(\beta) \qquad \text{for any } \alpha, \beta \in \mathbb{Z}[i]. \tag{9}$$

(This was a proposition in Lecture 7.)

We also observe that if α is a Gaussian integer satisfying $\alpha \neq 0$, then

$$N(\alpha) \text{ is a positive integer.} \tag{10}$$

[*Proof of* (10)*:* Let α be a Gaussian integer satisfying $\alpha \neq 0$. Then, $\alpha = a + bi$ for some $a, b \in \mathbb{Z}$ (since α is a Gaussian integer). Consider these a, b. We have $\alpha = a + bi$ (with $a, b \in \mathbb{Z}$) and thus $N(\alpha) = a^2 + b^2$ (by the definition of N). However, at least one of the two integers a and b is nonzero (since otherwise, we would have $a = 0$ and $b = 0$ and thus $\alpha = \underbrace{a}_{=0} + \underbrace{b}_{=0} i = 0$, contradicting $\alpha \neq 0$). Hence, at least one of the two nonnegative integers a and b is positive. Thus, $a^2 + b^2$ is a positive integer (being a sum of a nonnegative and a positive integer). In other words, $N(\alpha)$ is a positive integer (since $N(\alpha) = a^2 + b^2$). This proves (10).]

(a) Let z and w be two Gaussian integers satisfying $z \mid w$ in $\mathbb{Z}[i]$. From $z \mid w$, we see that there exists a $u \in \mathbb{Z}[i]$ such that $w = zu$. Consider this u. From $w = zu$, we obtain $N(w) = N(zu) = N(z)\,N(u)$ (by (9)). Since $N(u) \in \mathbb{N} \subseteq \mathbb{Z}$, this entails $N(z) \mid N(w)$ in $\mathbb{Z}$. This solves part **(a)** of the problem.

(b) Let w be a divisor of z in $\mathbb{Z}[i]$. Thus, $w \in \mathbb{Z}[i]$, so that we can write w in the form $w = c + di$ for some $c, d \in \mathbb{Z}$. Consider these c, d. We must thus prove that $c, d \in \{-n, -n+1, \ldots, n\}$.

We have $z = a + bi$ (with $a, b \in \mathbb{Z}$) and thus $N(z) = a^2 + b^2$ (by the definition of N). Also, $N(z)$ is a positive integer (by (10), applied to $\alpha = z$).

We have $w = c + di$ (with $c, d \in \mathbb{Z}$) and thus $N(w) = c^2 + d^2$ (by the definition of N). However, $w \mid z$ in $\mathbb{Z}[i]$ (since w is a divisor of z), and thus $N(w) \mid N(z)$ in $\mathbb{Z}$ (by part **(a)** of this exercise, applied to w and z instead of z and w). Since $N(z)$ is positive and $N(w)$ is nonnegative, this entails that $N(w) \leq N(z) = a^2 + b^2$.

Hence, $a^2 + b^2 \geq N(w) = c^2 + \underbrace{d^2}_{\geq 0} \geq c^2$. Since both sides of this inequality are nonnegative, we can take square roots and obtain $\sqrt{a^2+b^2} \geq \sqrt{c^2} = |c|$. Hence, $|c| \leq \sqrt{a^2+b^2}$. Therefore, $|c|$ is an integer that is $\leq \sqrt{a^2+b^2}$ (since $|c|$ is clearly an integer). Since $\left\lfloor \sqrt{a^2+b^2} \right\rfloor$ is the **largest** integer that is $\leq \sqrt{a^2+b^2}$, we thus conclude that $|c| \leq \left\lfloor \sqrt{a^2+b^2} \right\rfloor$. In other words, $|c| \leq n$ (since $n = \left\lfloor \sqrt{a^2+b^2} \right\rfloor$). Thus, $c \in \{-n, -n+1, \ldots, n\}$ (since c is an integer). A similar argument (using $\underbrace{c^2}_{\geq 0} + d^2 \geq d^2$ instead of $c^2 + \underbrace{d^2}_{\geq 0} \geq c^2$) shows that $d \in \{-n, -n+1, \ldots, n\}$. Thus, we have proved that $c, d \in \{-n, -n+1, \ldots, n\}$. Part **(b)** of the exercise is solved.

(d) See [19s, Proposition 4.2.9 **(b)**] for a proof of the equivalence (z is a unit of $\mathbb{Z}[i]$) $\iff$ ($N(z) = 1$), and see [19s, Proposition 4.2.10] for a proof of the equivalence (z is a unit of $\mathbb{Z}[i]$) $\iff$ ($z \in \{1, i, -1, -i\}$). (They are both rather easy: The first uses (9) and the fact that $N(z) = z\overline{z}$; the second uses the first along with the fact that two integers a, b satisfy $a^2 + b^2 = 1$ if and only if one of $|a|$ and $|b|$ is 0 and the other is 1.)

(c) We imitate the classical proof that every positive integer has a prime factorization:

We must prove that every nonzero $z \in \mathbb{Z}[i]$ has an irreducible factorization. We proceed by strong induction on $N(z)$ (using the fact that $N(z) \in \mathbb{N}$ for each $z \in \mathbb{Z}[i]$).

Induction step: Let $m \in \mathbb{N}$. Assume (as induction hypothesis) that every nonzero $z \in \mathbb{Z}[i]$ satisfying $N(z) < m$ has an irreducible factorization. We must show that every nonzero $z \in \mathbb{Z}[i]$ satisfying $N(z) = m$ has an irreducible factorization.

Indeed, let $z \in \mathbb{Z}[i]$ be nonzero and satisfy $N(z) = m$. We must prove that z has an irreducible factorization. If z is a unit, then this is obvious (because in this case, the empty list () is an irreducible factorization of z); it is also obvious if z is irreducible (since in this case, the list (z) is an irreducible factorization of z). Thus, for the rest of this proof, we WLOG assume that z is neither a unit nor irreducible. Hence, there exist $a, b \in \mathbb{Z}[i]$ such that $ab = z$ and such that neither a nor b is a unit (by the definition of "irreducible").[4] Consider these a, b.

[4]For constructivists or algorithmists, it is important to notice that all these distinctions and existence statements are constructive. Indeed, there is a simple algorithm for checking whether two Gaussian integers α and β satisfy $\alpha \mid \beta$ (namely, if $\alpha = 0$, then $\alpha \mid \beta$ holds if and only if $\beta = 0$; but otherwise, you can just compute the complex number $\dfrac{\beta}{\alpha} \in \mathbb{Q}[i]$ and check whether its real and imaginary part are integers). Thus, we can check whether z is a unit (indeed, z is a unit if and only if $z \mid 1$). Furthermore, part **(b)** of this exercise tells us that all divisors of z in $\mathbb{Z}[i]$ have the form $c + di$ for some $c, d \in \{-n, -n+1, \ldots, n\}$, where $n = \lfloor |z| \rfloor = \left\lfloor \sqrt{a^2+b^2} \right\rfloor$; thus, we can compute a list of all divisors of z in

From $ab = z$, we obtain $z = ab$ and thus $N(z) = N(ab) = N(a)\,N(b)$ (by (9)). Note that $z \neq 0$ (since z is nonzero); hence, $N(z)$ is a positive integer (by (10)). From $ab = z \neq 0$, we obtain $a \neq 0$. Hence, $N(a)$ is a positive integer (by (10)), and the Gaussian integer a is nonzero.

Part **(d)** of this exercise (applied to a instead of z) shows that we have the equivalence

$$(a \text{ is a unit of } \mathbb{Z}[i]) \iff (N(a) = 1) \iff (a \in \{1, i, -1, -i\}).$$

Hence, we don't have $N(a) = 1$ (since a is not a unit of $\mathbb{Z}[i]$). Thus, $N(a) \neq 1$, so that $N(a) > 1$ (since $N(a)$ is a positive integer). Likewise, $N(b) > 1$.

Now, from $N(a) > 1$ and $N(b) > 1$, we obtain $N(a)\,N(b) > N(a)$, so that $N(a) < N(a)\,N(b) = N(z)$ (since $N(z) = N(a)\,N(b)$). Thus, $N(a) < N(z) = m$. Hence, by our induction hypothesis, a has an irreducible factorization (since a is a nonzero element of $\mathbb{Z}[i]$). Similarly, b has an irreducible factorization. Let these two irreducible factorizations be $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$. Thus, $a \sim a_1 a_2 \cdots a_k$ and $b \sim b_1 b_2 \cdots b_\ell$. Hence, it is easy to see that $ab \sim a_1 a_2 \cdots a_k b_1 b_2 \cdots b_\ell$. Thus, ab has an irreducible factorization (namely, $(a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell)$). In other words, z has an irreducible factorization (since $z = ab$). This completes our induction step. Thus, part **(c)** of the exercise is solved.

---

7 Exercise 7

7.1 Problem

Consider the ring

$$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\right\}.$$

This ring is a subring of $\mathbb{C}$, and thus is an integral domain.

Let $u = 2 \in \mathbb{Z}\left[\sqrt{-3}\right]$ and $v = 1 + \sqrt{-3} \in \mathbb{Z}\left[\sqrt{-3}\right]$. Further let $a = 2u = 4$ and $b = 2v$.

(a) Prove that both u and v are common divisors of a and b in $\mathbb{Z}\left[\sqrt{-3}\right]$.

(b) Prove that the only divisors of 4 in $\mathbb{Z}\left[\sqrt{-3}\right]$ are ± 1, ± 2, ± 4, $\pm\left(1 + \sqrt{-3}\right)$, and $\pm\left(1 - \sqrt{-3}\right)$.

(c) Prove that a and b have no gcd in $\mathbb{Z}\left[\sqrt{-3}\right]$.

[**Hint:** For full credits on part **(b)**, it suffices to explain how the solution can be reduced to a finite computation and perform one representative case of the computation.]

7.2 Remark

This shows that $\mathbb{Z}\left[\sqrt{-3}\right]$ is not a UFD.

$\mathbb{Z}[i]$ (simply by running through all the $(2n+1)^2$ numbers of this form, and checking each of them for being a divisor of z). Thus, we can find all possible pairs (a, b) of Gaussian integers $a, b \in \mathbb{Z}[i]$ satisfying $ab = z$ (because both entries in such a pair (a, b) must be divisors of z in $\mathbb{Z}[i]$). This allows us to check whether z is irreducible, and, in case the answer is "no", to actually construct a pair (a, b) with $ab = z$ and such that neither a nor b is a unit.

7.3 Solution

...

---

8 Exercise 8

8.1 Problem

Let R be a ring. Let I and J be two ideals of R such that $I \subseteq J$. Let J/I denote the set of all cosets $j + I \in R/I$ where $j \in J$.

Prove the following:

(a) This set J/I is an ideal of R/I.

(b) We have $(R/I) / (J/I) \cong R/J$ (as rings). More concretely, there is a ring isomorphism $R/J \to (R/I) / (J/I)$ that sends each residue class $\overline{r} = r+J$ to $\overline{r+I} = (r+I)+(J/I)$.

8.2 Remark

This is known as the *Third Isomorphism Theorem for rings*.

For an example, take $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$ and $J = 2\mathbb{Z}$. In this case, J/I consists of the "even" residue classes $\overline{0}, \overline{2}, \overline{4}$ in $R/I = \mathbb{Z}/6$. Part **(b)** of the exercise says that if we "quotient them out" of $\mathbb{Z}/6$, then we are left with (an isomorphic copy of) $R/J = \mathbb{Z}/2$.

8.3 Solution

This can be solved in a pretty straightforward manner (i.e., checking the ideal axioms for part **(a)**, then constructing the isomorphism in part **(b)** and proving the requisite properties). However, here is a more elegant approach:

Consider the canonical projection

$$\begin{aligned} \pi_I : R &\to R/I, \\ r &\mapsto r + I. \end{aligned}$$

This projection π_I is a surjective ring morphism from R to R/I.

Consider the canonical projection

$$\begin{aligned} \pi_J : R &\to R/J, \\ r &\mapsto r + J. \end{aligned}$$

This projection π_J is a surjective ring morphism from R to R/J.

The definition of π_J shows that for each $i \in I$, we have $\pi_J(i) = i + J = 0$ (since $i \in I \subseteq J$). In other words, the map π_J sends each $i \in I$ to 0. In other words, $\pi_J(I) = 0$. Hence, the universal property of quotient rings (applied to $S = R/J$, $\pi = \pi_I$ and $f = \pi_J$) shows that there is a unique ring morphism $\pi'_J : R/I \to R/J$ satisfying $\pi_J = \pi'_J \circ \pi_I$.

Consider this π'_J. Thus, for each $r \in R$, we have

$$\begin{aligned} r + J &= \pi_J(r) && (\text{since } \pi_J(r) \text{ is defined to be } r + J) \\ &= (\pi'_J \circ \pi_I)(r) && (\text{since } \pi_J = \pi'_J \circ \pi_I) \\ &= \pi'_J\left(\underbrace{\pi_I(r)}_{\substack{=r+I \\ (\text{by the definition of } \pi_I)}}\right) \\ &= \pi'_J(r + I). \end{aligned} \tag{11}$$

Recall that π'_J is a ring morphism from R/I to R/J. Thus, the definition of $\operatorname{Ker}(\pi'_J)$ yields

$$\begin{aligned} \operatorname{Ker}(\pi'_J) &= \left\{a \in R/I \mid \pi'_J(a) = 0_{R/J}\right\} \\ &= \left\{ r + I \mid r \in R \text{ such that } \underbrace{\pi'_J(r + I)}_{\substack{=r+J \\ (\text{by (11)})}} = 0_{R/J} \right\} \\ &\qquad \left(\begin{array}{c} \text{here, we have substituted } r + I \text{ for } a, \text{ since every} \\ \text{element of } R/I \text{ has the form } r + I \text{ for some } r \in R \end{array}\right) \\ &= \left\{r + I \mid r \in R \text{ such that } r + J = 0_{R/J}\right\} \\ &= \{r + I \mid r \in J\} \qquad \left(\begin{array}{c} \text{since the elements } r \in R \text{ that satisfy } r + J = 0_{R/J} \\ \text{are precisely the elements of } J \end{array}\right) \\ &= \{j + I \mid j \in J\} \qquad (\text{here, we have renamed the index } r \text{ as } j) \\ &= J/I \qquad (\text{since } J/I \text{ was defined to be } \{j + I \mid j \in J\}). \end{aligned}$$

However, $\operatorname{Ker}(\pi'_J)$ is an ideal of R/I (since the kernel of a ring morphism is always an ideal of the domain). In other words, J/I is an ideal of R/I (since $\operatorname{Ker}(\pi'_J) = J/I$). This solves part **(a)** of the exercise.

(b) The morphism π'_J is surjective[5]. Thus,

$$\pi'_J(R/I) = R/J.$$

Now, π'_J is a ring morphism from R/I to R/J. Thus, the first isomorphism theorem (applied to R/I, R/J and π'_J instead of R, S and f) yields that we have

$$(R/I) / \operatorname{Ker}(\pi'_J) \cong \pi'_J(R/I), \tag{12}$$

and more precisely, the universal property of quotient rings yields a ring morphism

$$f' : (R/I) / \operatorname{Ker}(\pi'_J) \to R/J,$$

which (if we restrict its target to its actual image $\pi'_J(R/I)$) is a ring isomorphism from $(R/I) / \operatorname{Ker}(\pi'_J)$ to $\pi'_J(R/I)$. Consider this ring morphism f'.

[5] *Proof.* Let $u \in R/J$. Thus, $u = r + J$ for some $r \in R$. Consider this r. Hence, $u = r + J = \pi'_J(r + I)$ (by (11)). Thus, $u \in \pi'_J(R/I)$ (since $r + I \in R/I$).

Forget that we fixed u. We thus have shown that $u \in \pi'_J(R/I)$ for each $u \in R/J$. In other words, $R/J \subseteq \pi'_J(R/I)$. In other words, π'_J is surjective.

In view of $\operatorname{Ker}(\pi'_J) = J/I$ and $\pi'_J(R/I) = R/J$, we can rewrite (12) as $(R/I)/(J/I) \cong R/J$. Thus, we have shown that $(R/I)/(J/I) \cong R/J$ (as rings). It remains to prove the "More concretely" part of part **(b)** – i.e., to show that there is a ring isomorphism $R/J \to (R/I)/(J/I)$ that sends each residue class $\overline{r} = r + J$ to $\overline{r+I} = (r+I) + (J/I)$.

Let us consider the ring morphism f'. By its construction, it sends each residue class $u + \operatorname{Ker}(\pi'_J)$ to $\pi'_J(u)$. In other words, it satisfies

$$f'(u + \operatorname{Ker}(\pi'_J)) = \pi'_J(u) \tag{13}$$

for each $u \in R/I$. Hence, for each $r \in R$, we have

$$\begin{aligned} f'((r+I) + \operatorname{Ker}(\pi'_J)) &= \pi'_J(r+I) && \text{(by (13), applied to } u = r+I) \\ &= r + J && \text{(by (11))}. \end{aligned}$$

In view of $\operatorname{Ker}(\pi'_J) = J/I$, we can rewrite this as follows: For each $r \in R$, we have

$$f'((r+I) + (J/I)) = r + J. \tag{14}$$

Also, recall that the morphism f' (if we restrict its target to its actual image $\pi'_J(R/I)$) is a ring isomorphism from $(R/I)/\operatorname{Ker}(\pi'_J)$ to $\pi'_J(R/I)$. In view of $\operatorname{Ker}(\pi'_J) = J/I$ and $\pi'_J(R/I) = R/J$, we can restate this as follows: The morphism f' (if we restrict its target to its actual image R/J) is a ring isomorphism from $(R/I)/(J/I)$ to R/J.

Let $g : R/J \to (R/I)/(J/I)$ be the inverse of this ring isomorphism. Thus, from (14), we see that

$$g(r+J) = (r+I) + (J/I) \qquad \text{for each } r \in R.$$

In other words, g sends each residue class $r + J$ to $(r+I) + (J/I)$. Thus, we have found a ring isomorphism $R/J \to (R/I)/(J/I)$ that sends each residue class $r+J$ to $(r+I)+(J/I)$ (namely, the isomorphism g). This completes the solution to part **(b)** of the exercise.

---

9 Exercise 9

9.1 Problem

Let R be a ring. Let S be a subring of R. Let I be an ideal of R. Define $S + I$ to be the subset $\{s + i \mid s \in S \text{ and } i \in I\}$ of R.

Prove the following:

(a) This subset $S + I$ is a subring of R.

(b) The set I is an ideal of the ring $S + I$.

(c) The set $S \cap I$ is an ideal of the ring S.

(d) We have $(S+I)/I \cong S/(S \cap I)$ (as rings). More concretely, there is a ring isomorphism $S/(S \cap I) \to (S+I)/I$ that sends each residue class $\overline{s} = s + (S \cap I)$ to $\overline{s} = s + I$.

9.2 Remark

This is known as the *Second Isomorphism Theorem for rings.*

For an example, we can let

- R be the polynomial ring $\mathbb{Q}[x]$ of all univariate polynomials with rational coefficients;
- $I = \{a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid n \geq 0 \text{ and } a_i \in \mathbb{Q}\}$ be the ideal consisting of all polynomials divisible by x^2 (that is, all polynomials whose x^0-coefficient and x^1-coefficient are 0);
- S be the subring $\mathbb{Q}$ of R (which consists of all constant polynomials).

Then, $S + I = \{a_0 + a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid n \geq 0 \text{ and } a_i \in \mathbb{Q}\}$ is the set of all polynomials whose x^1-coefficient is 0. This is indeed a subring of R, as we have seen in Lecture 6 (where we have used this subring to find an irreducible element that is not prime).

9.3 Solution

...

---

10 Exercise 10

10.1 Problem

(a) Let R be a commutative ring, and let u and n be two nonnegative integers. Let $x, y \in R$ be two elements such that $x - y \in uR$. (Here, $uR := \{ur \mid r \in R\}$; this is a principal ideal of R, since $uR = (u1_R)\,R$.)

Prove that

$$x^n - y^n \in guR, \qquad \text{where } g = \gcd(n, u).$$

(b) Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence, defined as in Exercise 6 on homework set #1. Prove that

$$\gcd(n, f_d) \cdot f_d \mid f_{dn} \qquad \text{for any } d, n \in \mathbb{N}.$$

[**Hint:** For part **(a)**, write $x^n - y^n$ as $(x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})$, and show that the second factor belongs to gR. For part **(b)**, define the matrices A and B and the commutative ring $\mathcal{F}$ as in Exercise 6 on homework set #1, and apply part **(a)** to $x = A^d$ and $y = B^d$ and $u = f_d$.]

10.2 Solution

(a) Let $g = \gcd(n, u)$. Thus, $g = \gcd(n, u) \mid u$ and $g = \gcd(n, u) \mid n$. From $g \mid u$, we can easily obtain $uR \subseteq gR$ [6]. Similarly, from $g \mid n$, we obtain $nR \subseteq gR$.

[6] *Proof.* Let $a \in uR$. Thus, $a = ur$ for some $r \in R$. Consider this r. Now, $g \mid u$, so that $u = gc$ for some $c \in \mathbb{Z}$. Consider this c. We have $a = \underbrace{u}_{=gc} r = g \underbrace{cr}_{\in R} \in gR$.

Forget that we fixed a. We thus have shown that $a \in gR$ for each $a \in uR$. In other words, $uR \subseteq gR$.

Now, $x - y \in uR \subseteq gR$. Therefore, we have $\overline{x} = \overline{y}$ in the ring R/gR. Also, the map $R \to R/gR,\ a \mapsto \overline{a}$ is a ring morphism (indeed, this map is the canonical projection from R to R/gR), and thus preserves finite sums and powers. Hence, in R/gR, we have

$$\begin{aligned}\overline{x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}} &= \overline{x}^{n-1} + \overline{x}^{n-2}\overline{y} + \cdots + \overline{x}\,\overline{y}^{n-2} + \overline{y}^{n-1} \\ &= \sum_{k=0}^{n-1} \underbrace{\overline{x}^{n-1-k}\overline{y}^{k}}_{\substack{=\overline{y}^{n-1-k}\overline{y}^{k} \\ (\text{since } \overline{x}=\overline{y})}} = \sum_{k=0}^{n-1} \underbrace{\overline{y}^{n-1-k}\overline{y}^{k}}_{=\overline{y}^{n-1}} = \sum_{k=0}^{n-1} \overline{y}^{n-1} \\ &= n\overline{y}^{n-1} = \overline{ny^{n-1}} \end{aligned} \tag{15}$$

(again because the map $R \to R/gR,\ a \mapsto \overline{a}$ is a ring morphism). However, $n\underbrace{y^{n-1}}_{\in R} \in nR \subseteq gR$, so that $\overline{ny^{n-1}} = 0_{R/gR}$ in the ring R/gR. Hence, (15) becomes

$$\overline{x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}} = \overline{ny^{n-1}} = 0_{R/gR}.$$

In other words, $x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1} \in gR$. In other words, there exists some $r \in R$ such that

$$x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1} = gr.$$

Consider this r.

Also, there exists some $s \in R$ such that

$$x - y = us$$

(since $x - y \in uR$). Consider this s.

Now, $xy = yx$ (since R is commutative). Hence, a well-known formula says that

$$x^k - y^k = (x-y)\left(x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1}\right) \qquad \text{for each } k \in \mathbb{N}.$$

Applying this to $k = n$, we find

$$\begin{aligned} x^n - y^n &= \underbrace{(x-y)}_{=us}\underbrace{\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right)}_{=gr} \\ &= (us)(gr) = ug \cdot \underbrace{sr}_{\in R} \in \underbrace{ug}_{=gu} R = guR. \end{aligned}$$

This solves part **(a)** of the exercise.

(b) Define the matrices $A, B \in \mathcal{F}$ and the commutative ring $\mathcal{F}$ as in Exercise 6 on homework set #1. (Recall that $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ and $B = I_2 - A \in \mathbb{Z}^{2\times 2}$ and $\mathcal{F} = \{aA + bI_2 \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}^{2\times 2}$.)

We know that $A, B \in \mathcal{F}$ and thus $A - B \in \mathcal{F}$ (since $\mathcal{F}$ is a subring of $\mathbb{Z}^{2\times 2}$). Furthermore, Exercise 6 **(f)** on homework set #1 says that

$$A^n - B^n = f_n(A - B) \qquad \text{for all } n \in \mathbb{N}. \tag{16}$$

Now, let $d, n \in \mathbb{N}$. Set $g = \gcd(n, f_d)$. Then, (16) (applied to d instead of n) yields

$$A^d - B^d = f_d\underbrace{(A - B)}_{\in \mathcal{F}} \in f_d\mathcal{F}.$$

Hence, part **(a)** of the present exercise (applied to $R = \mathcal{F}$ and $x = A^d$ and $y = B^d$ and $u = f_d$) yields

$$\left(A^d\right)^n - \left(B^d\right)^n \in gf_d\mathcal{F} \qquad (\text{since } g = \gcd(n, f_d)).$$

In view of

$$\underbrace{\left(A^d\right)^n}_{=A^{dn}} - \underbrace{\left(B^d\right)^n}_{=B^{dn}} = A^{dn} - B^{dn} = f_{dn}(A - B) \qquad (\text{by (16), applied to } dn \text{ instead of } n),$$

this rewrites as

$$f_{dn}(A - B) \in gf_d\mathcal{F}.$$

In other words, there exists a matrix $\gamma \in \mathcal{F}$ such that

$$f_{dn}(A - B) = gf_d\gamma \tag{17}$$

(by the definition of $gf_d\mathcal{F}$). Consider this γ.

Since matrices are scaled entrywise, we have

$$\begin{aligned}&(\text{the } (2,2)\text{-th entry of the matrix } f_{dn}(A - B))\\ &= f_{dn} \cdot \underbrace{(\text{the } (2,2)\text{-th entry of the matrix } A - B)}_{=1} = f_{dn}.\end{aligned} \tag{18}$$

(this follows from a straightforward computation)

On the other hand, γ is a 2×2-matrix with integer entries (since $\gamma \in \mathcal{F} \subseteq \mathbb{Z}^{2\times 2}$). Hence, each entry of γ is an integer, i.e., belongs to $\mathbb{Z}$. Thus, in particular,

$$(\text{the } (2,2)\text{-th entry of the matrix } \gamma) \in \mathbb{Z}.$$

Now, (18) yields

$$\begin{aligned}f_{dn} &= (\text{the } (2,2)\text{-th entry of the matrix } f_{dn}(A - B))\\ &= (\text{the } (2,2)\text{-th entry of the matrix } gf_d\gamma) \qquad (\text{by (17)})\\ &= gf_d \cdot (\text{the } (2,2)\text{-th entry of the matrix } \gamma)\end{aligned}$$

(since matrices are scaled entrywise). This yields that $gf_d \mid f_{dn}$ (in the classical sense of divisibility of integers), because we know that (the $(2,2)$-th entry of the matrix γ) $\in \mathbb{Z}$. In other words, $\gcd(n, f_d) \cdot f_d \mid f_{dn}$ (since $g = \gcd(n, f_d)$). This solves part **(b)** of the exercise.

References

[19s] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 29 June 2019.
`http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf`

[DF] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 15 September 2022.
`http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`
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/2022-09-15c` .