Drexel University, Department of Mathematics

Math 533: Abstract Algebra I Winter 2021: Homework 2 student work

Exercise 1

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.

Solution. Let a be a nilpotent element of R and let $n \in \mathbb{N}$ be such that $a^n = 0$. Set $s = 1 + a + a^2 + a^3 + \cdots + a^{n-1} \in R$. Then,

$$\begin{aligned}
(1-a)s &= (1-a)(1+a+a^2+a^3+\cdots+a^{n-1}) \\
&= 1(1+a+a^2+a^3+\cdots+a^{n-1}) + (-a)(1+a+a^2+a^3+\cdots+a^{n-1}) \\
&= 1+a+a^2+a^3+\cdots+a^{n-1} - a - a^2 - a^3 - \cdots - a^{n-1} - a^n \\
&= 1 + a - a + a^2 - a^2 + a^3 - a^3 + \cdots + a^{n-1} - a^{n-1} - a^n \\
&= 1 + 0 + 0 + \cdots + 0 - a^n \\
&= 1 - a^n \\
&= 1 - 0 \qquad \text{(by assumption since } a^n = 0) \\
&= 1.
\end{aligned}$$

Similarly,

$$\begin{aligned}
s(1-a) &= (1+a+a^2+a^3+\cdots+a^{n-1})(1-a) \\
&= (1+a+a^2+a^3+\cdots+a^{n-1})1 + (1+a+a^2+a^3+\cdots+a^{n-1})(-a) \\
&= 1+a+a^2+a^3+\cdots+a^{n-1} - a - a^2 - a^3 - \cdots - a^{n-1} - a^n \\
&= 1 + a - a + a^2 - a^2 + a^3 - a^3 + \cdots + a^{n-1} - a^{n-1} - a^n \\
&= 1 + 0 + 0 + \cdots + 0 - a^n \\
&= 1 - a^n \\
&= 1 - 0 \qquad \text{(by assumption since } a^n = 0) \\
&= 1.
\end{aligned}$$

Hence $s \in R$ is a multiplicative inverse for $1 - a$. Thus $1 - a \in R$ is a unit.

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

Solution. Let a be a nilpotent element of R and $n \in \mathbb{N}$ be such that $a^n = 0$. Let $u \in R$ be a unit satisfying $ua = au$. Then $u^{-1} \in R$. Also, a commutes with u^{-1} (indeed, $ua = au \implies u^{-1}uau^{-1} = u^{-1}auu^{-1} \implies au^{-1} = u^{-1}a$). Hence, a commutes with u^{-k} for any $k \in \mathbb{N}$. Also, u commutes with a^k for any $k \in \mathbb{N}$ (since $au = ua$).

Define $t = u^{-1} + au^{-2} + a^2u^{-3} + \cdots + a^{n-2}u^{-n+1} + a^{n-1}u^{-n} \in R$. Then,

$$\begin{aligned}
(u-a)t &= (u-a)(u^{-1} + au^{-2} + a^2u^{-3} + \cdots + a^{n-2}u^{-n+1} + a^{n-1}u^{-n}) \\
&= u(u^{-1} + au^{-2} + a^2u^{-3} + \cdots + a^{n-2}u^{-n+1} + a^{n-1}u^{-n}) \\
&\qquad + (-a)(u^{-1} + au^{-2} + a^2u^{-3} + \cdots + a^{n-2}u^{-n+1} + a^{n-1}u^{-n}) \\
&= 1 + au^{-1} + a^2u^{-2} + \cdots + a^{n-2}u^{-n+2} + a^{n-1}u^{-n+1} \\
&\qquad - au^{-1} - a^2u^{-2} - a^3u^{-3} - \cdots - a^{n-1}u^{-n+1} - a^nu^{-n} \\
&\qquad\qquad \text{(because } u \text{ commutes with } a^k \text{ for any } k \in \mathbb{N}) \\
&= 1 + 0 + 0 + 0 + \cdots + 0 - a^nu^{-n} \\
&= 1 - 0u^{-n} \qquad \text{(since by assumption } a^n = 0) \\
&= 1 - 0
\end{aligned}$$

$$= 1.$$

Similarly,

$$\begin{aligned}
t(u-a) &= (u^{-1} + au^{-2} + a^2u^{-3} + \cdots + a^{n-2}u^{-n+1} + a^{n-1}u^{-n})(u-a) \\
&= (u^{-1} + au^{-2} + a^2u^{-3} + \cdots + a^{n-2}u^{-n+1} + a^{n-1}u^{-n})u \\
&\qquad + (u^{-1} + au^{-2} + a^2u^{-3} + \cdots + a^{n-2}u^{-n+1} + a^{n-1}u^{-n})(-a) \\
&= 1 + au^{-1} + a^2u^{-2} + \cdots + a^{n-2}u^{-n+2} + a^{n-1}u^{-n+1} \\
&\qquad - au^{-1} - a^2u^{-2} - a^3u^{-3} - \cdots - a^{n-1}u^{-n+1} - a^nu^{-n} \\
&\qquad\qquad \big(\text{because } a \text{ commutes with } u^{-k} \text{ for any } k \in \mathbb{N}\big) \\
&= 1 + 0 + 0 + 0 + \cdots + 0 - a^nu^{-n} \\
&= 1 - 0u^{-n} \qquad (\text{since by assumption } a^n = 0) \\
&= 1 - 0 \\
&= 1.
\end{aligned}$$

Hence $t \in R$ is a multiplicative inverse for $u - a$. Thus $u - a \in R$ is a unit.

Exercise 2

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

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

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

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

Solution. Addition: As the addition is the same as the original ring $(R, +, \cdot)$ and so are the elements, clearly $(R, +, 0_R)$ is still an abelian group.

Multiplication: The neutral element 1_R is inherited from the original ring; it remains neutral for the new multiplication $\widetilde{\cdot}$, since it commuted with all elements of R.

Associativity: For any $a, b, c \in R$, we have

$$\begin{aligned} a \widetilde{\cdot} (b \widetilde{\cdot} c) &= a \widetilde{\cdot} (cb) \\ &= (cb)a \\ &= c(ba) \qquad \text{(by associativity of the original multiplication)} \\ &= c(a \widetilde{\cdot} b) \\ &= (a \widetilde{\cdot} b) \widetilde{\cdot} c. \end{aligned}$$

Thus the new multiplication $\widetilde{\cdot}$ is associative. Distributivity: For any $a, b, c \in R$, we have

$$\begin{aligned} (a + b) \widetilde{\cdot} c &= c(a + b) \\ &= ca + cb \qquad \text{(by distributivity in the original ring)} \\ &= a \widetilde{\cdot} c + b \widetilde{\cdot} c. \end{aligned}$$

The other direction is analogous. Thus, the new multiplication $\widetilde{\cdot}$ satisfies distributivity.

Multiplication by 0: We don't strictly need to check the $0_R \widetilde{\cdot} a = a \widetilde{\cdot} 0_R = 0_R$ axiom, but of course we can (it follows from the corresponding axiom in the original ring).

Altogether, $(R, +, \widetilde{\cdot})$ 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 $\text{id} : R \to R$ is a ring isomorphism from R to R^{op} if and only if R is commutative.

Solution. (I) Suppose R is commutative. We shall show $\text{id} : R \to R$ is a ring isomorphism from R to R^{op}. For any $a, b \in R$ we have

Addition: $\text{id}(a + b) = a + b = \text{id}(a) + \text{id}(b)$.

Zero: $\text{id}(0_R) = 0_R = 0_{R^{\text{op}}}$.

Multiplication: $\text{id}(ab) = ab = ba = a \widetilde{\cdot} b = \text{id}(a) \widetilde{\cdot} \text{id}(b)$ since R is commutative.

Unity: $\text{id}(1_R) = 1_R = 1_{R^{\text{op}}}$.

Invertibility: The identity map is clearly one-to-one and onto; thus invertible.

Altogether, the identity map is a ring isomorphism from R to R^{op}.

(II) Suppose $\text{id} : R \to R$ is a ring isomorphism from R to R^{op}. Then, for all elements $a, b \in R$, we have $\text{id}(ab) = \text{id}(a) \widetilde{\cdot} \text{id}(b)$. Thus

$$ab = a \widetilde{\cdot} b = ba.$$

Hence R is commutative.

(I) and (II) together show the identity map $\text{id} : R \to R$ 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.

Solution. Define $f : R \to R^{\mathrm{op}}$ by $f(A) = A^T$. We shall show this is a ring isomorphism. (Note I use 0 to represent the 0 matrix and I to represent the identity matrix; these two matrices are the additive and multiplicative identities, respectively, for both rings.) For any $A, B \in R$, we have

<u>Addition:</u> $f(A+B) = (A+B)^T = A^T + B^T = f(A) + f(B)$.

<u>Zero:</u> $f(0) = 0^T = 0$.

<u>Multiplication:</u>

$$\begin{aligned} f(AB) &= (AB)^T \\ &= B^T A^T \qquad \text{(a classical property of transposes, which relies on the commutativity of } S\text{)} \\ &= A^T \,\tilde{\cdot}\, B^T = f(A) \,\tilde{\cdot}\, f(B). \end{aligned}$$

<u>Unity:</u> $f(I) = I^T = I$.

<u>Invertibility:</u> The map f is its own inverse. (This follows from the fact that $(A^T)^T = A$ for any matrix A.)

Altogether, we have that f 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.)

Solution. Since M is a right R-module, we must already have that $(M, +, 0_M)$ is an abelian group.

Next, for any $r, s \in R$ (thus also all $r, s \in R^{\mathrm{op}}$) and $m, n \in M$, we have

<u>Right Distributivity:</u> $(r+s)m = m(r+s) = mr + ms = rm + sm$ by left distributivity in the right R-module M.

<u>Left Distributivity:</u> $r(m+n) = (m+n)r = mr + nr = rm + rn$ by right distributivity in the right R-module M.

<u>Associativity:</u>

$$\begin{aligned} (r \,\tilde{\cdot}\, s)m &= (sr)m \qquad \text{(by definition of } \tilde{\cdot}\text{)} \\ &= m(sr) \\ &= (ms)r \qquad \text{(by associativity in the right } R\text{-module } M\text{)} \\ &= (sm)r \\ &= r(sm). \end{aligned}$$

The facts that $0_R m = 0_M$, $r 0_M = 0_M$, and $1m = m$ follow from M being a right R-module.

Altogether, we have that M is a left R^{op}-module.

Exercise 3

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 $g\ell = ab$.

Solution. The ring R is an integral domain; thus, it is commutative and has no zero divisors.

Trivial Case: If $a = 0$, then ℓ, being a multiple of a, is also 0. Thus, in this case, b is a gcd of a and b and satisfies $b\ell = ab$ (since $\ell = 0 = a$). This solves the problem in the case when $a = 0$. Similarly we can solve the problem if $b = 0$.

Now assume a and b are nonzero. Thus, $ab \neq 0$ (since R is an integral domain). There exist $m_1, m_2 \in R$ such that

$$am_1 = \ell \qquad \text{and} \qquad bm_2 = \ell$$

(since ℓ is a common multiple of a and b). Next, note that ab is a common multiple of a and b. Since ℓ is an lcm of a and b, we thus conclude that there exists an element $g \in R$ such that $\ell g = ab$. We want to show that this element g is a gcd of a and b.

Note that $\ell g = ab \neq 0$, so that $\ell \neq 0$.

Step 1: Show that g is a common divisor of a and b.

We have $\ell g = ab$ and $am_1 = \ell$. This gives

$$\begin{aligned} am_1 g &= ab; \\ am_1 g - ab &= 0; \\ a(m_1 g - b) &= 0; \\ m_1 g - b &= 0 \qquad (\text{since } R \text{ has no zero divisors and } a \neq 0); \\ m_1 g &= b. \end{aligned}$$

Hence $g \mid b$.

Similarly, we have $\ell g = ab$ and $bm_2 = \ell$. This gives

$$\begin{aligned} bm_2 g &= ab; \\ bm_2 g - ab &= 0; \\ b(m_2 g - a) &= 0 \qquad (\text{since } R \text{ is commutative}); \\ m_2 g - a &= 0 \qquad (\text{since } R \text{ has no zero divisors and } b \neq 0); \\ m_2 g &= a. \end{aligned}$$

Hence $g \mid a$. Thus together, g is a common divisor of a and b.

Step 2: Show that every common divisor of a and b divides g.

Let d be a common divisor of a and b. Thus for some $n_1, n_2 \in R$, we have

$$dn_1 = a \qquad \text{and} \qquad dn_2 = b.$$

Then, $dn_1 n_2$ is a common multiple of a and b (indeed, it equals an_2 and $n_1 b$ by commutativity of the ring R). Since ℓ is an lcm of a and b, we thus conclude that there exists $k \in R$ such that $\ell k = dn_1 n_2$. Next, from $dn_1 = a$ and $dn_2 = b$, we obtain $(dn_1)(dn_2) = ab = \ell g$. However, since R is commutative, we have $(dn_1)(dn_2) = d(dn_1 n_2) = d\ell k$ (because $dn_1 n_2 = \ell k$). Comparing these two equalities, we find

$$\begin{aligned} d\ell k &= \ell g; \\ d\ell k - \ell g &= 0; \\ \ell(dk - g) &= 0 \qquad (\text{since } R \text{ is commutative}); \\ dk - g &= 0 \qquad (\text{since } R \text{ has no zero divisors and } \ell \neq 0); \\ dk &= g. \end{aligned}$$

Hence d divides g. Since d was an arbitrary common divisor of a and b, every common divisor of a and b divides g.

Steps 1 and 2 together show that g is a gcd of a and b. Furthermore, it satisfies $g\ell = ab$.

Exercise 4

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 $a \equiv b \equiv 0 \mod p$.

Solution (sketched). First assume $p \neq 2$. Suppose a and b are two integers such that $a^2 \equiv b^2 \mod p^2$. This gives that $p^2 \mid (a^2 - b^2)$. Then since $a^2 - b^2 = (a+b)(a-b)$ and p is prime, we have three options:[1]

Option 1: $p^2 \mid (a+b)$. Thus $a \equiv -b \mod p^2$.

Option 2: $p^2 \mid (a-b)$. Thus $a \equiv b \mod p^2$.

Option 3: $p \mid (a-b)$ and $p \mid (a+b)$. Then, there exist integers n_1 and n_2 such that

$$a - b = pn_1 \qquad \text{and} \qquad a + b = pn_2.$$

Adding these equalities, we get $2a = p(n_1 + n_2)$. Since 2 divides the left-hand side, it must divide the right-hand side. Since p is odd, we thus find $2 \mid (n_1 + n_2)$, so that $m = \dfrac{n_1 + n_2}{2} \in \mathbb{Z}$. Hence $a = pm$ for an integer m, so $a \equiv 0 \mod p$. Then, since $p \mid (a-b) \implies a \equiv b \mod p$, we also get $b \equiv 0 \mod p$. Altogether we have

$$a \equiv b \equiv 0 \mod p.$$

Hence we have shown that one of the following must hold:

$$(1)\ a \equiv b \mod p^2 \qquad \text{or} \qquad (2)\ a \equiv -b \mod p^2 \qquad \text{or} \qquad (3)\ a \equiv b \equiv 0 \mod p.$$

Now let's prove this in the $p = 2$ case. Suppose a and b are two integers such that $a^2 \equiv b^2 \mod 4$. If a is even, then b must also be even. In this case $a \equiv b \equiv 0 \mod 2$. Else, a is odd, in which case b is also odd. Every odd number is one less or one more than a multiple of four. Thus we have four cases:

Case 1: $a = 4k + 1$ and $b = 4l + 1$ for some $k, l \in \mathbb{Z}$.

Case 2: $a = 4k - 1$ and $b = 4l - 1$ for some $k, l \in \mathbb{Z}$.

Case 3: $a = 4k + 1$ and $b = 4l - 1$ for some $k, l \in \mathbb{Z}$.

Case 4: $a = 4k - 1$ and $b = 4l + 1$ for some $k, l \in \mathbb{Z}$.

Cases 1 and 2 give $a \equiv b \mod 4$ whereas cases 3 and 4 give $a \equiv -b \mod 4$. Thus whenever $a^2 \equiv b^2 \mod 4$, we have one of the following:

$$(1)\ a \equiv b \mod 4 \qquad \text{or} \qquad (2)\ a \equiv -b \mod 4 \qquad \text{or} \qquad (3)\ a \equiv b \equiv 0 \mod 2.$$

In total, we have shown the statement for all prime p.

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

Solution (sketched). First, squaring any multiple of p in $\mathbb{Z}/p^2$ will give 0. Thus we want to take out the multiples of p, of which there are p (including 0) in $\mathbb{Z}/p^2$. This takes care of the case when $a \equiv b \equiv 0 \mod p$. Then, of the remaining elements of $\mathbb{Z}/p^2$, any two distinct elements, say $\overline{a}$ and $\overline{b}$, will give the same square if and only if $\overline{a} = \overline{-b}$ in $\mathbb{Z}/p^2$ (i.e. $a \equiv -b \mod p^2$).

Why must $\overline{a}$ and $\overline{b}$ be distinct? Suppose $a \equiv -a \mod p^2$. Then, for some integer k, we have $a + a = p^2 k$, i.e., $2a = p^2 k$. Since 2 divides the lefthand side, it must also divide the righthand side. Since 2 is prime, $2 \mid p$ or $2 \mid k$. In either case, $2 \mid pk$. Then for $l = \frac{pk}{2} \in \mathbb{Z}$, we have $a = pl$. Thus $a \equiv 0 \mod p$. But this was the first case we took care of, so we have reached a contradiction. Hence, $\overline{a}$ and $\overline{b}$ must be distinct.

Thus the number of squares in $\mathbb{Z}/p^2$ is given by

$$\underbrace{1}_{\text{(corresponding to the square 0)}} + \underbrace{\frac{|\mathbb{Z}/p^2| - p}{2}}_{\text{exactly two non-multiples of } p \text{ will give the same square}} = 1 + \frac{p^2 - p}{2} = \frac{p^2 - p + 2}{2}.$$

(A generalization of **(b)** is found in [1].)

[1] *Remark by Darij:* Make sure you understand why! (Hint: Any integer not divisible by p is coprime to p and thus also coprime to p^2.)

Exercise 5

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 $\overline{-1}$.

Solution. Suppose $m \in \mathbb{Z}/p$ is its own inverse. Then $m \cdot m = \overline{1}$. Thus we have

$$\begin{aligned} m^2 &= \overline{1}; \\ m^2 + \overline{-1} &= \overline{0}; \\ m^2 + m - m + \overline{-1} &= \overline{0}; \\ m(m+\overline{1}) + \overline{-1}(m+\overline{1}) &= \overline{0}; \\ (m+\overline{-1})(m+\overline{1}) &= \overline{0}. \end{aligned}$$

Since p is prime, $\mathbb{Z}/p$ is a field, so there are no zero divisors. Thus we have either

$$m + \overline{-1} = \overline{0} \implies m = \overline{1}$$

or

$$m + \overline{1} = \overline{0} \implies m = \overline{-1}.$$

Hence the only elements of $\mathbb{Z}/p$ that are their own inverses are $\overline{1}$ and $\overline{-1}$.

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

Solution. Wilson's theorem ([2]) gives us that $(p-1)! \equiv -1 \mod p$, i.e. that in $\mathbb{Z}/p$, we have

$$\overline{1} \cdot \overline{2} \cdot \overline{3} \cdots \overline{p-2} \cdot \overline{p-1} = \overline{-1}.$$

Manipulating this (using $u+1 = p-u$), we get:

$$\begin{aligned} \overline{1} \cdot \overline{2} \cdots \overline{u} \cdot \overline{p-u} \cdots \overline{p-2} \cdot \overline{p-1} &= \overline{-1}; \\ \overline{1} \cdot \overline{2} \cdots \overline{u} \cdot \overline{-u} \cdots \overline{-2} \cdot \overline{-1} &= \overline{-1}; \\ \overline{1} \cdot \overline{2} \cdots \overline{u} \cdot \overline{-1}^u \cdot \overline{u} \cdots \overline{2} \cdot \overline{1} &= \overline{-1}; \\ \overline{-1}^u (\overline{1} \cdot \overline{2} \cdots \overline{u})^2 &= \overline{-1}; \\ \overline{-1}^u \cdot \overline{-1}^u (\overline{1} \cdot \overline{2} \cdots \overline{u})^2 &= \overline{-1}^u \cdot \overline{-1}; \\ (\overline{1} \cdot \overline{2} \cdots \overline{u})^2 &= \overline{-1} \cdot \overline{-1}^u. \end{aligned}$$

Thus we have shown that $(u!)^2 \equiv -(-1)^u \mod p$.

Exercise 6

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 $\mathbb{Z}$.

Solution. Suppose $z = a_1 + b_1 i$ and $w = a_2 + b_2 i$ (where $a_1, a_2, b_1, b_2 \in \mathbb{Z}$) satisfy $z \mid w$. Since we have $z \mid w$, there exists $r = c + di \in \mathbb{Z}[i]$ such that $zr = w$. Thus we have

$$(a_1 + b_1 i)(c + di) = a_2 + b_2 i;$$
$$(a_1 c - b_1 d) + (a_1 d + b_1 c)i = a_2 + b_2 i.$$

Hence

$$a_1 c - b_1 d = a_2 \qquad \text{and} \qquad a_1 d + b_1 c = b_2.$$

Thus,

$$\begin{aligned} a_2^2 + b_2^2 &= (a_1 c - b_1 d)^2 + (a_1 d + b_1 c)^2 \\ &= a_1^2 c^2 - 2a_1 c b_1 d + b_1^2 d^2 + a_1^2 d^2 + 2a_1 c b_1 d + b_1^2 c^2 \\ &= a_1^2 c^2 + b_1^2 d^2 + a_1^2 d^2 + b_1^2 c^2 \\ &= a_1^2 (c^2 + d^2) + b_1^2 (c^2 + d^2) \\ &= (a_1^2 + b_1^2)(c^2 + d^2). \end{aligned}$$

Since $r = c + di \in \mathbb{Z}[i]$, we have $c, d \in \mathbb{Z}$ and thus $c^2 + d^2 \in \mathbb{Z}$. Hence

$$(a_1^2 + b_1^2) \mid (a_2^2 + b_2^2).$$

Now $N(z) = N(a_1 + b_1 i) = a_1^2 + b_1^2$ and $N(w) = N(a_2 + b_2 i) = a_2^2 + b_2^2$. Thus altogether we have

$$N(z) \mid N(w).$$

(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 $c, d \in \{-n, -n+1, \ldots, n\}$.

Solution. Part (a) tells us that any divisor $v = c + di$ of $z = a + bi$ in $\mathbb{Z}[i]$ must satisfy $N(v) \mid N(z)$, i.e. that

$$(c^2 + d^2) \mid (a^2 + b^2).$$

Since both quantities are nonnegative, and since $a^2 + b^2 > 0$ (because $z \neq 0$), we have then that

$$c^2 + d^2 \leq a^2 + b^2;$$
$$\sqrt{c^2 + d^2} \leq \sqrt{a^2 + b^2}.$$

Since $|c| \leq \sqrt{c^2 + d^2}$ and $|d| \leq \sqrt{c^2 + d^2}$, we thus obtain

$$-\sqrt{a^2 + b^2} \leq c \leq \sqrt{a^2 + b^2} \qquad \text{and} \qquad -\sqrt{a^2 + b^2} \leq d \leq \sqrt{a^2 + b^2}.$$

Since $v = c + di \in \mathbb{Z}[i]$, we have $c, d \in \mathbb{Z}$. Hence we get that $c, d \in \{-n, -n+1, \ldots, n\}$. Thus we have shown 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.

Solution omitted.

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

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

Solution. Step 1: z is a unit of $\mathbb{Z}[i] \implies N(z) = 1$.

Proof. Suppose z is a unit of $\mathbb{Z}[i]$. Then $z \mid 1$. By part (a), we get $N(z) \mid N(1)$. Thus if $z = a + bi$

where $a, b \in \mathbb{Z}$, then $(a^2 + b^2) \mid 1$ (in the normal $\mathbb{Z}$ division sense). This will only happen if $a^2 + b^2 = 1$ since a and b are real and thus $a^2 + b^2 \geq 0$. Thus $N(z) = 1$.

Step 2: $N(z) = 1 \implies z \in \{1, i, -1, -i\}$.

Proof. Suppose $N(z) = 1$. Then, if we write $z = a + bi$ where $a, b \in \mathbb{Z}$, then $a^2 + b^2 = 1$. Since a and b are integers, this equality only holds if one of a^2 and b^2 is 0 and the other is 1. Thus we get the following cases:

1. $b^2 = 0$ and $a^2 = 1$:
   - 1.1 $b = 0$ and $a = 1$. Thus $z = 1$.
   - 1.2 $b = 0$ and $a = -1$. Thus $z = -1$.
2. $b^2 = 1$ and $a^2 = 0$:
   - 2.1 $b = 1$ and $a = 0$. Thus $z = i$.
   - 2.2 $b = -1$ and $a = 0$. Thus $z = -i$.

Hence $z \in \{1, i, -1, -i\}$.

Step 3: $z \in \{1, i, -1, -i\} \implies N(z) = 1$.

Proof. Suppose $z \in \{1, i, -1, -i\}$. In all cases $N(z) = a^2 + b^2 = 0 + 1 = 1$.

Step 4: $N(z) = 1 \implies z$ is a unit of $\mathbb{Z}[i]$.

Proof. Suppose $N(z) = 1$. By step 2, $z \in \{1, i, -1, -i\}$. In all cases, z is a unit:

a. If $z = 1$, its inverse is itself.
b. If $z = i$, its inverse is $-i \in \mathbb{Z}[i]$.
c. If $z = -1$, its inverse is itself.
d. If $z = -i$, its inverse is $i \in \mathbb{Z}[i]$.

Hence z is a unit of $\mathbb{Z}[i]$.

The four steps above have proven the equivalences:

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

Exercise 7

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 $\mathbb{Z}\left[\sqrt{-3}\right]$.

Solution. It is clear that $u \mid a = 2u$. Let's show $v \mid a$: For $r = 1 - \sqrt{-3} \in \mathbb{Z}\left[\sqrt{-3}\right]$,

$$\begin{aligned} vr &= (1+\sqrt{-3})(1-\sqrt{-3}) \\ &= 1 - \sqrt{-3}\sqrt{-3} \\ &= 1 - (-3) \\ &= 1 + 3 \\ &= 4 \\ &= a. \end{aligned}$$

Hence $v \mid a$ in $\mathbb{Z}\left[\sqrt{-3}\right]$.

Next, it is clear that $v \mid b = 2v$ and also that $u = 2 \mid b = 2v$. Thus since u and v both divide a in $\mathbb{Z}\left[\sqrt{-3}\right]$ and they both divide b in $\mathbb{Z}\left[\sqrt{-3}\right]$, they 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 $\pm\left(1-\sqrt{-3}\right)$.

Note in this part I will use $\gcd_{\mathbb{Z}}$ to denote the usual gcd in the integer setting. This gcd is always a nonnegative integer.

Solution. Suppose $c + d\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ (with $c, d \in \mathbb{Z}$) satisfies $(c + d\sqrt{-3}) \mid 4 = a$. Then,

$$\frac{4}{c + d\sqrt{-3}} \in \mathbb{Z}[\sqrt{-3}].$$

Rationalizing the denominator, we find

$$\frac{4}{c+d\sqrt{-3}} = \frac{4}{c+d\sqrt{-3}} \cdot \frac{c-d\sqrt{-3}}{c-d\sqrt{-3}} = \frac{4(c-d\sqrt{-3})}{c^2+3d^2} = \frac{4c}{c^2+3d^2} - \frac{4d}{c^2+3d^2}\sqrt{-3},$$

so that

$$\frac{4c}{c^2+3d^2} - \frac{4d}{c^2+3d^2}\sqrt{-3} = \frac{4}{c+d\sqrt{-3}} \in \mathbb{Z}[\sqrt{-3}].$$

In other words,

$$\frac{4c}{c^2+3d^2} \in \mathbb{Z} \qquad \text{and} \qquad \frac{4d}{c^2+3d^2} \in \mathbb{Z}.$$

That is, $c^2 + 3d^2$ is a common divisor of $4c$ and $4d$ (over the integers). Therefore, $(c^2 + 3d^2) \mid \gcd_{\mathbb{Z}}(4c, 4d)$. Set $\gcd_{\mathbb{Z}}(c, d) = g \in \mathbb{Z}$ (so that $\gcd_{\mathbb{Z}}(4c, 4d) = 4g$), and let $k, l \in \mathbb{Z}$ such that $c = kg$ and $d = lg$. Then we have

$$\begin{aligned} (c^2+3d^2) &\mid 4g; \\ (|c|^2+3|d|^2) &\mid 4g; \\ (|ckg|+3|dlg|) &\mid 4g \qquad \text{(since } c = kg \text{ and } d = lg\text{)}; \\ |g|(|kc|+3|ld|) &\mid 4g; \\ (|kc|+3|ld|) &\mid 4 \end{aligned}$$

(here, we cancelled out $|g|$, which is legitimate since it is easily seen that $g \neq 0$). Since $k, c, l, d \in \mathbb{Z}$, we thus have two cases: either $|ld| = 1$ or $|ld| = 0$ (since otherwise $|kc| + 3|ld| > 4$, which is a contradiction to $(|kc| + 3|ld|) \mid 4$):

1. If $|ld| = 1$, then $|d| = 1$ and $(|kc| + 3) \mid 4$, so we have $|kc| = 1$. This means also $|c| = 1$, so we get the following divisors of 4:

(a) $d = 1$, $c = 1$: $1 + \sqrt{-3}$.
(b) $d = 1$, $c = -1$: $-1 + \sqrt{-3}$.
(c) $d = -1$, $c = 1$: $1 - \sqrt{-3}$.
(d) $d = -1$, $c = -1$: $-1 - \sqrt{-3}$.

2. If $|ld| = 0$, then $d = 0$ (since $d = lg$ yields $|d|^2 = |dlg| = |ld||g| = 0$). Further, $|kc| \mid 4$, so we have $c \mid 4$, which gives the following (familiar) divisors of 4:
   (a) ± 1.
   (b) ± 2.
   (c) ± 4.

Thus all the divisors of $a = 4$ in $\mathbb{Z}[\sqrt{-3}]$ 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 $\mathbb{Z}\left[\sqrt{-3}\right]$.

Solution. A gcd of a and b must be a common divisor of a and b, so first let's check which of the divisors of $a = 4$ (which we have found above, in part **(b)** of the exercise) are also divisors of $b = 2(1 + \sqrt{-3})$:

1. It is clear that ± 1, ± 2, and $\pm(1 + \sqrt{-3})$ are divisors of b.
2. It is clear that ± 4 are **not** divisors of b since

$$\frac{b}{4} = \frac{2(1 + \sqrt{-3})}{4} = \frac{1}{2} + \frac{1}{2}\sqrt{-3} \notin \mathbb{Z}[\sqrt{-3}].$$

3. It remains to check $\pm(1 - \sqrt{-3})$. Note:

$$(1 - \sqrt{-3})(-1 + \sqrt{-3}) = -1 + \sqrt{-3} + \sqrt{-3} + 3 = 2 + 2\sqrt{-3} = b.$$

   Thus $\pm(1 - \sqrt{-3})$ are divisors of b.

In all we have that the common divisors of a and b are

$$\pm 1, \pm 2, \pm\left(1 + \sqrt{-3}\right), \pm\left(1 - \sqrt{-3}\right).$$

Thus if a and b have a gcd it would be one of the above. Every common divisor must divide the gcd. In particular, since 2 is a common divisor of a and b, it must divide the gcd. It is clear that in $\mathbb{Z}[\sqrt{-3}]$, 2 does not divide any of

$$\pm 1, \pm\left(1 + \sqrt{-3}\right), \pm\left(1 - \sqrt{-3}\right),$$

since in each case dividing by 2 over the complex numbers will yield a real part of $\pm\frac{1}{2} \notin \mathbb{Z}$. Thus our only remaining options for gcd of a and b are ± 2. If ± 2 is the gcd, $1 + \sqrt{-3}$ must divide it. We have

$$\frac{\pm 2}{1 + \sqrt{-3}} = \frac{\pm 2}{1 + \sqrt{-3}} \cdot \frac{1 - \sqrt{-3}}{1 - \sqrt{-3}} = \frac{\pm 2(1 - \sqrt{-3})}{1 + 3} = \frac{\pm 1}{2}(1 - \sqrt{-3}) \notin \mathbb{Z}[\sqrt{-3}].$$

Thus ± 2 cannot be the gcd either. Hence a and b have no gcd in $\mathbb{Z}[\sqrt{-3}]$.

Exercise 8

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.

Solution. Step 1: We need to show that any $\alpha, \beta \in J/I$ satisfy $\alpha + \beta \in J/I$.

Let $\alpha, \beta \in J/I$. Then, we can write $\alpha = a + I$ and $\beta = b + I$ for some $a, b \in J$. Since J is an ideal of R, we then have $a + b \in J$. Thus $(a + b) + I \in J/I$. But this is precisely how we define $(a + I) + (b + I)$. Thus $(a + I) + (b + I) \in J/I$. In other words, $\alpha + \beta \in J/I$. This shows that J/I is closed under addition.

Step 2: We need to show that any $\alpha \in R/I$ and $\beta \in J/I$ satisfy $\alpha\beta \in J/I$ and $\beta\alpha \in J/I$.

Let $\alpha \in R/I$ and $\beta \in J/I$. Thus we can write $\alpha = a + I$ and $\beta = j + I$ with $a \in R$ and $j \in J$. Since J is an ideal of R, we then have $aj \in J$ and $ja \in J$. Thus $aj + I \in J/I$ and $ja + I \in J/I$. This is precisely how we define $(a + I)(j + I)$ and $(j + I)(a + I)$, respectively. Thus $(a + I)(j + I) \in J/I$ and $(j + I)(a + I) \in J/I$. In other words, $\alpha\beta \in J/I$ and $\beta\alpha \in J/I$. This shows that J/I is closed under multiplication by elements in R/I.

Step 3: We need to show that $0_R + I = 0_{R/I} \in J/I$.

Since J is an ideal, $0_R \in J$. Thus $0_R + I \in J/I$.

All steps above show that 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 $\overline{r + I} = (r + I) + (J/I)$.

Solution. We want to show that $f : R/J \to (R/I) / (J/I)$ defined by

$$f(r + J) = (r + I) + (J/I)$$

is a ring isomorphism.

Well-definedness: If $r + J$ and $s + J$ (for some $r, s \in R$) are one and the same coset in R/J, then $(r + I) + (J/I) = (s + I) + (J/I)$. Indeed, in this case, we have $r - s \in J$ (since $r + J = s + J$) and therefore $(r + I) - (s + I) = (r - s) + I \in J/I$,, so that $(r + I) + (J/I) = (s + I) + (J/I)$. Thus, the map f above is well-defined.

Addition: For any $r + J, s + J \in R/J$, we have[2]

$$\begin{aligned} f((r + J) + (s + J)) &= f((r + s) + J) \\ &= \Big([r + s] + I\Big) + (J/I) \\ &= \Big([r + I] + [s + I]\Big) + (J/I) \qquad \text{(by definition of coset sum)} \\ &= \Big[(r + I) + (J/I)\Big] + \Big[(s + I) + (J/I)\Big] \qquad \text{(by definition of coset sum)} \\ &= f(r + J) + f(s + J). \end{aligned}$$

Multiplication: For any $r + J, s + J \in R/J$,

$$\begin{aligned} f((r + J)(s + J)) &= f((rs) + J) \\ &= \Big([rs] + I\Big) + (J/I) \\ &= \Big([r + I][s + I]\Big) + (J/I) \qquad \text{(by definition of coset multiplication)} \\ &= \Big[(r + I) + (J/I)\Big]\Big[(s + I) + (J/I)\Big] \qquad \text{(by definition of coset multiplication)} \\ &= f(r + J)f(s + J). \end{aligned}$$

Zero: $f(0_{R/J}) = f(0_R + J) = (0_R + I) + (J/I) = 0_{R/I} + (J/I) = 0_{(R/I)/(J/I)}$.

[2] We shall use square brackets synonymously to regular parentheses.

Unity: $f(1_{R/J}) = f(1_R + J) = (1_R + I) + (J/I) = 1_{R/I} + (J/I) = 1_{(R/I)/(J/I)}$.

Invertible: We will show that f is injective and surjective. This will then yield that f is invertible.

Injective: Suppose $f(a) = f(b)$ for some $a, b \in R/J$. Then $a = r + J$ and $b = s + J$ for some $r, s \in R$. Thus we have $f(r + J) = f(s + J)$ for some $r + J, s + J \in R/J$. Then by definition of f we have

$$(r + I) + (J/I) = (s + I) + (J/I).$$

This means that $(r+I)-(s+I) \in J/I$, i.e. $(r-s)+I \in J/I$. This means that $(r-s)+I = j+I$ for some $j \in J$. This yields $(r - s) - j \in I \subseteq J$, so that $r - s$ is a sum of j with an element of J. Thus, $r - s$ is a sum of two elements of J (since $j \in J$). Therefore, $r - s \in J$ (since J is an ideal). In other words, $r + J = s + J$. Hence $a = b$. Thus we have shown that f is injective.

Surjective: Let $y \in (R/I)/(J/I)$. Then for some $r \in R$, we have $y = (r+I)+(J/I) \in (R/I)/(J/I)$. Since $r \in R$, we have $r + J \in R/J$ and

$$f(r + J) = (r + I) + (J/I) = y.$$

Hence f is surjective.

All the above together gives that f is an invertible ring morphism, i.e., a ring isomorphism. Hence $(R/I) / (J/I) \cong R/J$ (as rings).

Exercise 9

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.

Solution. Closed under Addition: Let $a, b \in S+I$ be arbitrary. Then for some $s_1, s_2 \in S$ and $i_1, i_2 \in I$, we have $a = s_1 + i_1$ and $b = s_2 + i_2$. Then

$$\begin{aligned} a+b &= s_1 + i_1 + s_2 + i_2 \\ &= (s_1+s_2) + (i_1+i_2) \\ &= s_3 + i_3 \end{aligned}$$

for $s_3 = s_1 + s_2 \in S$ and $i_3 = i_1 + i_2 \in I$ since S is a subring (thus closed under addition) and I is an ideal (thus also closed under addition). Hence $a+b = s_3 + i_3 \in S+I$. Thus $S+I$ is closed under addition.

Closed under Multiplication: Let $a, b \in S+I$ be arbitrary. Then for some $s_1, s_2 \in S$ and $i_1, i_2 \in I$, we have $a = s_1 + i_1$ and $b = s_2 + i_2$. Then

$$\begin{aligned} ab &= (s_1+i_1)(s_2+i_2) \\ &= (s_1+i_1)s_2 + (s_1+i_1)i_2 \\ &= s_1s_2 + i_1s_2 + s_1i_2 + i_1i_2. \end{aligned}$$

Since I is an ideal it is closed under multiplication by any element of R (and thus any element of S), so $i_1s_2, s_1i_2, i_1i_2 \in I$. Therefore $i_3 = i_1s_2 + s_1i_2 + i_1i_2 \in I$. On the other hand, S, as a subring, is closed under multiplication. Thus $s_3 = s_1s_2 \in S$. Therefore we have

$$ab = s_3 + i_3 \qquad \text{where } s_3 \in S \text{ and } i_3 \in I.$$

Hence $S+I$ is closed under multiplication.

Contains Additive Inverses: Let $a \in S+I$ be arbitrary. Then for some $s \in S$ and $i \in I$, we have $a = s+i$. Then

$$-a = -(s+i) = -s + (-i).$$

Since S is a subring of R, we have $-s \in S$. Since I is an ideal of R, it is closed under multiplication by elements of R. Thus $-i = (-1)i \in I$. Hence we have that $-a = -s + (-i) \in S+I$. Thus $S+I$ contains additive inverses.

Zero: $0_R \in S$ as S is a subring and $0_R \in I$ as I is an ideal. Thus $0_R = 0_R + 0_R \in S+I$.

Unity: $1_R \in S$ as S is a subring and $0_R \in I$ as I is an ideal. Thus $1_R = 1_R + 0_R \in S+I$.

All of the above shows that $S+I$ is a subring of R.

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

Solution. Clearly $I \subseteq S+I$, since each $i \in I$ satisfies $i = 0_R + i$ with $0_R \in S$. The rest of the claim follows from I being an ideal of R and $S+I$ being a subring of R. In fact, certainly I is still closed under addition, closed under multiplication by elements of $S+I$ (since they are also elements of R) and contains the 0 of $S+I$ since it is the same as the 0 of R.

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

Solution. Clearly $S \cap I \subseteq S$.

Closed under Addition: Since S is a subring and I an ideal, they are both closed under addition. Hence we get that $S \cap I$ is also closed under addition.

Closed Under Multiplication by Elements of S: Let $a \in S \cap I$ be arbitrary. Then $a \in S$ and $a \in I$. For any $b \in S$, we have $ab \in S$ and $ba \in S$ since S is a ring (by part (**a**)) and thus closed under multiplication. Further, $b \in R$ since $S \subseteq R$. Thus $ab \in I$ and $ba \in I$ since I is an ideal of R and thus closed under multiplication by elements of R. Altogether we have that $ab \in S \cap I$ and $ba \in S \cap I$. Hence we have that $S \cap I$ is closed under multiplication by elements in S.

Zero: Since $0_S \in S$ and $0_S = 0_R \in I$, we have that $0_S \in S \cap I$.

All of the above shows that $S \cap I$ is an ideal of 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 $\overline{s} = s + I$.

Solution. We want to show that $f : S/(S\cap I) \to (S+I)/I$ defined by

$$f(s + (S\cap I)) = s + I$$

is a ring isomorphism.

Well-definedness: If $r + (S\cap I)$ and $s + (S\cap I)$ (for some $r, s \in S$) are one and the same coset in $S/(S\cap I)$, then $r+I = s+I$. Indeed, in this case, we have $r-s \in S\cap I$ (since $r+(S\cap I) = s+(S\cap I)$) and therefore $r - s \in I$, so that $r + I = s + I$. Thus, the map f above is well-defined.

Addition: For any $s + (S\cap I), r + (S\cap I) \in S/(S\cap I)$,

$$\begin{aligned} f((s + (S\cap I)) + (r + (S\cap I))) &= f((s+r) + (S\cap I)) \\ &= (s+r) + I \\ &= (s+I) + (r+I) \qquad \text{(by definition of coset sum)} \\ &= f(s + (S\cap I)) + f(r + (S\cap I)). \end{aligned}$$

Multiplication: For any $s + (S\cap I), r + (S\cap I) \in S/(S\cap I)$,

$$\begin{aligned} f((s + (S\cap I))(r + (S\cap I))) &= f((sr) + (S\cap I)) \\ &= (sr) + I \\ &= (s+I)(r+I) \qquad \text{(by definition of coset multiplication)} \\ &= f(s + (S\cap I))f(r + (S\cap I)). \end{aligned}$$

Zero: $f(0_{S/(S\cap I)}) = f(0_S + (S\cap I)) = f(0_R + (S\cap I)) = 0_R + I = 0_{S+I} + I = 0_{(S+I)/I}$.

Unity: $f(1_{S/(S\cap I)}) = f(1_S + (S\cap I)) = f(1_R + (S\cap I)) = 1_R + I = 1_{S+I} + I = 1_{(S+I)/I}$.

Invertible: We will show that f is injective and surjective. This will then yield that f is invertible.

Injective: Suppose $f(a) = f(b)$ for some $a, b \in S/(S\cap I)$. Then $a = s+(S\cap I)$ and $b = r+(S\cap I)$ for some $r, s \in S$. Thus we have $f(s+(S\cap I)) = f(r+(S\cap I))$ for some $s+(S\cap I), r+(S\cap I) \in S/(S\cap I)$. Then by definition of f we have

$$s + I = r + I.$$

This means that $s - r \in I$. Since $r, s \in S$, which is a ring, we also have $s - r \in S$. Thus $s - r \in S \cap I$. Therefore $s + (S\cap I) = r + (S\cap I)$. Hence $a = b$. This shows that f is injective.

Surjective: Let $y \in (S+I)/I$. Then for some $r \in S + I$, we have $y = r + I \in (S+I)/I$. Since $r \in S + I$, for some $s \in S$ and $i \in I$, we have $r = s + i$. Thus

$$y = (s+i) + I = (s+I) + (i+I) = (s+I) + (0+I) = s + I.$$

Since $s \in S$, we have $s + (S\cap I) \in S/(S\cap I)$ and

$$f(s + (S\cap I)) = s + I = y.$$

Hence f is surjective.

All the above together gives that f is an invertible ring morphism, i.e., a ring isomorphism. Hence $(S+I)/I \cong S/(S\cap I)$ (as rings).

References

[1] Stangl, Walter D. (1996). Counting Squares in $\mathbb{Z}_n$. *Mathematics Magazine, 69*(4), 285-289. https://doi.org/10.1080/0025570X.1996.11996456

[2] Wikipedia contributors, Wilson's Theorem, *Wikipedia, The Free Encyclopedia*, https://en.wikipedia.org/wiki/Wilson's_theorem .