Quotient ring of R modulo I

Question.....

$$R/I = \{r+I \mid r \in R\}$$

Proposition

Let R be a (possibly nonunital) ring and let $I \subseteq R$ be an ideal. Then the set

$$R/I = \{r+I \mid r \in R\}$$

forms a (possibly nonunital) quotient ring, with addition and multiplication operations

- $(r+I)+(s+I) = (r+s)+I$
- $(r+I)\cdot(s+I) = (r\cdot s)+I$

for any $r, s \in R$.

Furthermore, if R is unital, so is R/I, and if R is commutative, R/I is as well.

Proof: Exercise.

Example 1@

Let $f_n : \mathbb{Z} \to \mathbb{Z}_n$ be the ring homomorphism given by

$$f_n(k) = [k]_n$$

Then the kernel $K = \ker(f_n)$ is an

ideal of $\mathbb{Z}$ and we can therefore form the quotient ring $\mathbb{Z}/K$.

$$K = \ker(f_n) = \{x \in \mathbb{Z} \mid f_n(x) = [0]_n\}$$
$$= \{x \in \mathbb{Z} \mid [x]_n = [0]_n\}$$
$$= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{n}\}$$
$$= \{x \in \mathbb{Z} \mid x = kn \text{ for some } k \in \mathbb{Z}\}$$
$$= \{kn \text{ for some } k \mathbb{Z}\}$$
$$= \langle n \rangle$$
$$= n\mathbb{Z}$$

The kernel K consists of all integers congruent to 0 modulo n; that is all integers of the form kn.

A coset $m + K$ therefore consists of integers of the form $m + kn$; that is, exactly those integers that are congruent to m modulo n. There are thus n of these, namely

$K = 0 + K$,
$1 + K$,
...
$(n-1) + K$.

The quotient ring $\mathbb{Z}/K = \mathbb{Z}/n\mathbb{Z}$ therefore consists of these n cosets.

Its additive structure is exactly addition modulo n, and its multiplicative structure is multiplication modulo n. Hence $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Observe that f_n is a surjective homomorphism so that

$$\text{im}(f_n) = \mathbb{Z}_n$$

The example above shows that

$$\mathbb{Z}/\text{Ker}(f_n) \cong \text{im}(f_n),$$

which is a ring-theoretic example of the First Isomorphism Theorem for groups.

Example 1(b)

$\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$

To see how to add and multiply, consider $2+4\mathbb{Z}$ and $3+4\mathbb{Z}$

$$(2+4\mathbb{Z})+(3+4\mathbb{Z}) = 5+4\mathbb{Z}$$
$$= 1+4+4\mathbb{Z}$$
$$= 1+4\mathbb{Z},$$

$$(2+4\mathbb{Z})(3+4\mathbb{Z}) = 6+4\mathbb{Z}$$
$$= 2+4+4\mathbb{Z}$$
$$= 2+4\mathbb{Z}$$

Do not write in this margin

Question.....

One can readily see that the two operations are essentially modulo 4 arithmetic.

Example 1 ©

$2\mathbb{Z}/6\mathbb{Z} = \{0+6\mathbb{Z}, 2+6\mathbb{Z}, 4+6\mathbb{Z}\}$

Addition in $2\mathbb{Z}/6\mathbb{Z}$:

$$(4+6\mathbb{Z})+(4+6\mathbb{Z}) = 8+6\mathbb{Z}$$
$$= 2+6+6\mathbb{Z}$$
$$= 2+6\mathbb{Z}$$

Multiplication in $2\mathbb{Z}/6\mathbb{Z}$:

$$(4+6\mathbb{Z})(4+6\mathbb{Z}) = 16+6\mathbb{Z}$$
$$= 4+6+6+6\mathbb{Z}$$
$$= 4+6\mathbb{Z}$$

Here, the operations are essentially modulo 6 arithmetic.

Example 2 Consider the ring homomorphisms $f: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2$ and $g: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_3$ ~~such that~~ given by

$$f(k) = \begin{cases} 0 & \text{if } k = 0,2,4 \\ 1 & \text{if } k = 1,3,5 \end{cases}$$

and

$$g(k) = \begin{cases} 0 & \text{if } k = 0,3 \\ 1 & \text{if } k = 1,4 \\ 2 & \text{if } k = 2,5 \end{cases}$$

Question.....

$K_1 = \ker(f) = \{0, 2, 4\}$

and

$K_2 = \ker(g) = \{0, 3\}$

The cosets of K_1 in $\mathbb{Z}_6$ are

$K_1 = 0 + K_1 = 2 + K_1 = 4 + K_1 = \{0, 2, 4\}$

and $1 + K_1 = 3 + K_1 = 5 + K_1 = \{1, 3, 5\}$

The quotient ring $\mathbb{Z}_6/K_1$ thus has 2 elements and must therefore be isomorphic to $\mathbb{Z}_2$. By examining the addition and multiplication of these cosets, we find that this is indeed the case.

+	K_1	$1+K_1$
K_1		
$1+K_1$		

·	K_1	$1+K_1$
K_1		
$1+K_1$		

The cosets of K_2 in $\mathbb{Z}_6$ are

$K_2 = 0 + K_2 = 3 + K_2 = \{0, 3\}$,

$1 + K_2 = 4 + K_2 = \{1, 4\}$,

and $2 + K_2 = 5 + K_2 = \{2, 5\}$

Question.....

There are 3 of these, and hence the quotient ring $\mathbb{Z}_6/K_2$ has 3 elements and must be isomorphic to $\mathbb{Z}_3$; examination of the additive and multiplicative structure confirms this.

+	K_2	$1+K_2$	$2+K_2$
K_2			
$1+K_2$			
$2+K_2$			

·	K_2	$1+K_2$	$2+K_2$
K_2			
$1+K_2$			
$2+K_2$			

Question.....

Example 3

Let $R = \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \middle| a_i \in \mathbb{Z} \right\}$

and let I be the subset of R consisting of matrices with even entries.
It is easy to show that I is indeed an ideal of R (Exercise).

(quotient)
Consider the factor ring R/I.
What is its size?

We claim R/I has 16 elements; in fact,

$$R/I = \left\{ \begin{pmatrix} r_1 & r_2 \\ r_3 & r_4 \end{pmatrix} + I \middle| r_i \in \{0, 1\} \right\}.$$

An example illustrates the typical situation.
Which of the 16 elements is $\begin{pmatrix} 7 & 8 \\ 5 & -3 \end{pmatrix} + I$?

Observe that

$$\begin{pmatrix} 7 & 8 \\ 5 & -3 \end{pmatrix} + I = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 6 & 8 \\ 4 & -4 \end{pmatrix} + I$$

$$= \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + I,$$

since an ideal absorbs its own elements.

Example 4.

Let $\mathbb{Z}[x]$ denote the ring of polynomials in x over $\mathbb{Z}$, and let $\langle 2 \rangle$ be the principal ideal generated by 2; this consists of all polynomials with even integer coefficients. The cosets of $\langle 2 \rangle$ in $\mathbb{Z}[x]$ are all of the form $p + \langle 2 \rangle$, where $p(x) = a_0 + a_1 x + \dots + a_n x^n$, with $a_0, a_1, \dots, a_n \in \{0, 1\}$.

Hence the quotient ring $\mathbb{Z}[x]/\langle 2 \rangle$ consists of the cosets determined by finite-degree polynomials in x with coefficients all equal to either 0 or 1.

By considering the additive and multiplicative structure of these cosets, it turns out that

$$\mathbb{Z}[x]/\langle 2 \rangle \cong \mathbb{Z}_2[x],$$

the ring of polynomials in x over $\mathbb{Z}_2$.

In this example, factoring by the ideal $\langle 2 \rangle$ has the effect of setting 2 equal to 0, but leaving x and its powers unchanged. This results in a change of coefficient ring from $\mathbb{Z}$ to $\mathbb{Z}_2$.

Question.....

Example 5

We can factor the ring $\mathbb{Z}[x]$ by more complicated ideals.

In particular, $I = \langle x^2+1 \rangle$ consists of all polynomials over $\mathbb{Z}$ which have (x^2+1) as a factor.

In the quotient $\mathbb{Z}[x]/\langle x^2+1 \rangle$, two polynomials are equivalent if they differ by a multiple of x^2+1.

Also, since $x^2+1=0$, we have $x^2=-1$

This means that any $p \in \mathbb{Z}[x]$ maps in the quotient $\mathbb{Z}[x]/\langle x^2+1 \rangle$ to the corresponding polynomial with every x^2 replaced by a -1. For example, $x^6+3x^5+2x^2-1$ maps to $(-1)^3+3x(-1)^2+2(-1)-1$

$$= 3x-4$$

The cosets in $\mathbb{Z}[x]/\langle x^2+1 \rangle$ are thus all of the form

$$(a+bx)+I,$$

where $a, b \in \mathbb{Z}$.

Their additive structure:

$$\big((a+bx)+I\big)+\big((c+dx)+I\big)=\big((a+c)+(b+d)x\big)+I$$

for any $a, b, c, d \in \mathbb{Z}$.

Question.....

Do not write in this margin

The multiplicative structure is interesting and somewhat familiar:

$$\begin{aligned}((a+bx)+I)\cdot((c+dx)+I) &= ((a+bx)\cdot(c+dx))+I \\ &= (ac+(ad+bc)x+bdx^2)+I \\ &= ((ac-bd)+(ad+bc)x)+I\end{aligned}$$

In fact, the quotient ring $\mathbb{Z}[x]/\langle x^2+1\rangle$ is isomorphic to the ring $\mathbb{Z}[i]$ of ~~gaxxx~~ Gaussian integers, via the isomorphism

$$(a+bx)+I \longmapsto a+bi$$

Example 6

Consider the quotient ring of the Gaussian integers $R=\mathbb{Z}[i]/\langle 2-i\rangle$.

What does this ring look like?
The elements of R are of the form $a+bi+\langle 2-i\rangle$, where $a,b\in\mathbb{Z}$.

What do the distinct cosets look like?
The fact that

$$2-i+\langle 2-i\rangle = 0+\langle 2-i\rangle$$

Question.....

means that, when dealing with coset representatives, we may treat $2-i$ as equivalent to 0, so that $2 = i$.

For example,

the coset $3 + 4i + \langle 2+i \rangle$

$= 3 + 4(2) + \langle 2 - i \rangle$

$= 3 + 8 + \langle 2 - i \rangle$

$= 11 + \langle 2 - i \rangle$.

Similarly, all the elements of R can be written in the form,

$a + \langle 2 - i \rangle$,

where $a \in \mathbb{Z}$.

We can further reduce the set of distinct coset representatives by observing that when dealing with coset representatives, $2 = i$ implies that $4 = -1$ or $5 = 0$.

Thus, the coset $3 + 4i + \langle 2 - i \rangle$

$= 11 + \langle 2 - i \rangle$

$= 1 + 5 + 5 + \langle 2 - i \rangle$

$= 1 + \langle 2 - i \rangle$

In this way, we can show that every element of R is equal to one of the following cosets:

$0 + \langle 2 - i \rangle$, $1 + \langle 2 - i \rangle$, $2 + \langle 2 - i \rangle$, $3 + \langle 2 - i \rangle$, $4 + \langle 2 - i \rangle$.

Is any further reduction possible?
To demonstrate that there is not, we will show that these 5 cosets are distinct.
It suffices to show that
$1+\langle 2-i\rangle$ has additive order 5.

Since $5(1+\langle 2-i\rangle) = 5+\langle 2-i\rangle$
$= 0+\langle 2-i\rangle$,
$1+\langle 2-i\rangle$ has order 1 or 5.
If the order is actually 1, then
$1+\langle 2-i\rangle = 0+\langle 2-i\rangle$,
so $1 \in \langle 2-i\rangle$.
Thus $1 = (2-i)(a+bi)$
$= 2a+b+(-a+2b)i$
for some integers a and b.
But this equation implies that

$$1 = 2a+b$$

and

$$0 = -a+2b,$$

and solving these simultaneously,

$$b = 1/5,$$

which is a contradiction.
It should be clear that the ring R is essentially the same as the field $\mathbb{Z}_5$.

Question.....

Question

How many elements are there in the quotient ring $\mathbb{Z}[i] / \langle 3+i \rangle$?

Justify your answer.

Question.....

ISOMORPHISM THEOREMS FOR RINGS

Theorem (First Isomorphism Theorem)

Let $f: R \longrightarrow S$ be a (possibly nonunital) ring homomorphism, and let $K = \ker(f)$. Then the function

$$\phi: R/K \longrightarrow \text{im}(f)$$

given by

$$\phi(r+K) = f(r)$$

is an isomorphism.

That is,

$$R/\ker(f) \cong \text{im}(f).$$

Proof

We need to show that ϕ is a well-defined function, a ring homomorphism, and a bijection.

Suppose that $a, b \in R$ such that

$$a+K = b+K.$$

Then $(a-b)$ must lie in the kernel K, and hence $f(a-b)$ lies in the image $f(K) = \{0\}$.

Hence $f(a-b) = 0$,

and since f is a ring homomorphism,

$$0 = f(a-b) = f(a) - f(b),$$

therefore

$$f(a) = f(b)$$

So if $a+K = b+K$, it follows that

$$\begin{aligned}\phi(a+K) &= f(a) \\ &= f(b) \\ &= \phi(b+K),\end{aligned}$$

and thus ϕ is well-defined.

Next we have to check that ϕ is a ring homomorphism.

Firstly,

$$\begin{aligned}\phi((a+K)+(b+K)) &= \phi((a+b)+K) \\ &= f(a+b) \\ &= f(a)+f(b) \\ &= \phi(a+K)+\phi(b+K)\end{aligned}$$

and secondly,

$$\begin{aligned}\phi((a+K)\cdot(b+K)) &= \phi((a\cdot b)+K) \\ &= f(a\cdot b) \\ &= f(a)f(b) \\ &= \phi(a+K)\cdot\phi(b+K)\end{aligned}$$

Do not write in this margin

Question.....

Every element of $\text{im}(f)$ is of the form $\phi(a+K)$ for some coset $(a+K) \in R/K$, so ϕ is surjective.

To see that ϕ is injective, suppose that $\phi(a+K) = \phi(b+K)$ for some $a, b \in R$.

Then

$$\begin{aligned} 0 &= \phi(a+K) - \phi(b+K) \\ &= f(a) - f(b) \\ &= f(a-b) \end{aligned}$$

and hence $(a-b) \in \ker(f)$, which means that

$$a+K = b+K,$$

and therefore ϕ is injective.

Thus $\phi: R/K \longrightarrow \text{im}(f)$ is a well-defined ring isomorphism.

There are ring-theoretic versions of the Second and Third Isomorphism Theorems.

First we need some preliminary facts about ideals and subrings.

Question.....

Here, and in what follows, for some subring S and ideal I in a ring R, we set

$$S+I = \{ s+i \mid s \in S, i \in I \}$$

Proposition

Let R be a (unital or nonunital) ring, let S be a (possibly nonunital) subring of R, and let I be an ideal of R. Then

(i) $S+I$ is a (possibly nonunital) subring of R;

(ii) $S \cap I$ is an ideal of S, and

(iii) I is an ideal of $S+I$.

Question

Theorem (Second Isomorphism Theorem)

Let R be a ring and let I be an ideal of R. Then

$$(R+I)/I \cong R/(R \cap I)$$

Proof

$f : R \longrightarrow (R+I)/I$

$r \longmapsto r+I$

ring homo? ✓

$\cdot \ker(f) = R \cap I$

Theorem (Third Isomorphism Theorem)

Let R be a ring, and let I and J be ideals of R such that $I \subseteq J$. Then

$$(R/J)/(I/J) \cong R/I$$

Proof

$f : R/J \longrightarrow R/I$

$a+J \longmapsto a+I$

$\cdot$ well-defined

$\cdot$ ring homo

$\cdot \ker f = I/J$

$\cdot \operatorname{im} f = \{a+I \mid a \in R\} = R/I$