Visual Algebra

Lecture 8.5: The ring isomorphism theorems

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

The isomorphism theorems for rings

All of the isomorphism theorems for groups have analogues for rings.

- Fundamental homomorphism theorem: "*All homomorphic images are quotients*"
- Correspondence theorem: Characterizes "*subrings and ideals of quotients*"
- Fraction theorem: Characterizes "*quotients of quotients*"
- Diamond theorem: Characterizes "*duality of subquotients*"

Since rings are abelian groups with extra structure, we don't have to prove these from scratch.

FHT for rings

If $\phi\colon R \to S$ is a ring homomorphism, then $R/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$.

Proof (sketch)

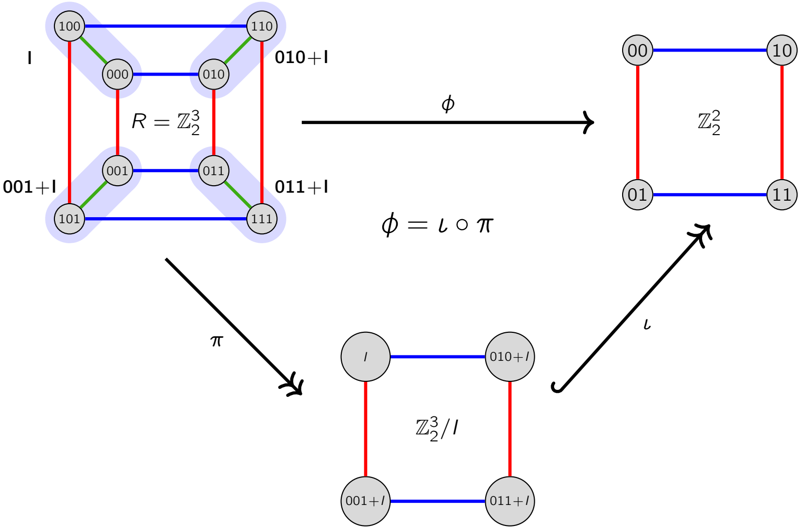
The statement holds for the underlying additive group $(R, +)$. Thus, it remains to show that the relabeling map (a group isomorphism)

$$\iota\colon R/I \longrightarrow \operatorname{Im}(\phi)\,, \qquad\qquad \iota(r+I) = \phi(r).$$

is also a ring homomorphism.

The FHT for rings

Consider the ring homomorphism $\phi\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^2$, $\qquad \phi\colon abc \longmapsto bc$.



The FHT for rings

Consider the ring homomorphism $\phi\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^2$, $\quad \phi\colon abc \longmapsto bc$.

By the FHT for groups, we know that $\mathbb{Z}_2^3/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi) = \mathbb{Z}_2^2$, as (additive) groups.

+	000	100	010	110	001	101	011	111
000	000	100	010	110	001	101	011	111
100	100	000	110	010	101	001	111	011
010	010	110	000	100	011	111	001	101
110	110	010	100	000	111	011	101	001
001	001	101	011	111	000	100	010	110
101	101	001	111	011	100	000	110	010
011	011	111	001	101	010	110	000	100
111	111	011	101	001	110	010	100	000

000+I	010+I	001+I	011+I
010+I	000+I	011+I	001+I
001+I	011+I	000+I	010+I
011+I	001+I	010+I	000+I

$\xrightarrow{\ \iota\ }$

+	000	100	010	110	001	101	011	111
000	000	100	010	110	001	101	011	111
100	100	000	110	010	101	001	111	011
010	010	110	000	100	011	111	001	101
110	110	010	100	000	111	011	101	001
001	001	101	011	111	000	100	010	110
101	101	001	111	011	100	000	110	010
011	011	111	001	101	010	110	000	100
111	111	011	101	001	110	010	100	000

-00	-10	-01	-11
-10	-00	-11	-01
-01	-11	-00	-10
-11	-01	-10	-00

The image is isomorphic to the Klein 4-group

$$\mathbb{Z}_2^2 \cong \{\underbrace{(0,0)}_{0}, \underbrace{(1,0)}_{a}, \underbrace{(0,1)}_{b}, \underbrace{(1,1)}_{c}\}.$$

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

+	00	10	01	11
00	00	10	01	11
10	10	00	11	01
01	01	11	00	10
11	11	01	10	00

The FHT theorem for rings says that ι also preserves the multiplicative structure of R/I.

The FHT for rings

Consider the ring homomorphism $\phi\colon \mathbb{Z}_2^3 \longrightarrow \mathbb{Z}_2^2, \qquad \phi\colon abc \longmapsto bc.$

The following Cayley tables show how ι preserves the multiplicative structure:

$$\iota\big((r+I)(s+I)\big) = \iota(rs+I).$$

×	000	100	010	110	001	101	011	111
000	000	000	000	000	000	000	000	000
100	000	100	000	100	000	100	000	100
010	000	000	010	010	000	000	010	010
110	000	100	010	110	000	100	010	110
001	000	000	000	000	001	001	001	001
101	000	100	000	100	001	101	001	101
011	000	000	010	010	001	001	011	011
111	000	100	010	110	001	101	011	111

Labels printed over the 2×2 blocks of the left table:

000+I	000+I	000+I	000+I
000+I	010+I	000+I	010+I
000+I	000+I	001+I	001+I
000+I	010+I	001+I	011+I

$\xrightarrow{\ \iota\ }$

The right table has the same header row, row labels and small entries as the left table. Labels printed over its 2×2 blocks:

-00	-00	-00	-00
-00	-10	-00	-10
-00	-00	-01	-01
-00	-10	-01	-11

This quotient ring is isomorphic to

$$\left\{ \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}_{0}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}}_{a}, \underbrace{\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}}_{b}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{c} \right\}.$$

×	0	a	b	c
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
c	0	a	b	c

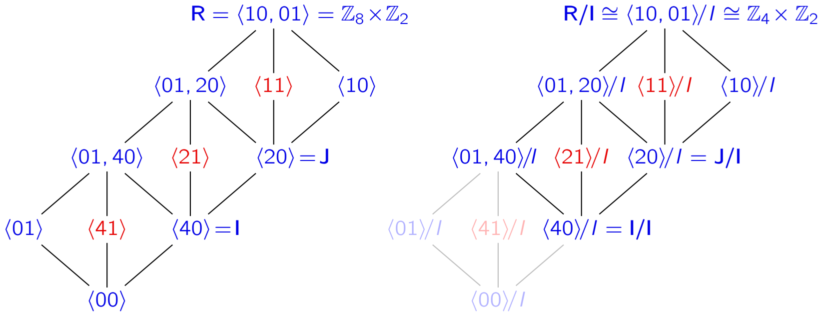
×	00	10	01	11
00	00	00	00	00
10	00	10	00	10
01	00	00	01	01
11	00	10	01	11

The correspondence theorem: subrings of quotients

Correspondence theorem

Let I be an ideal of R. There is a bijective correspondence between subrings of R/I and subrings of R that contain I.

Moreover every ideal of R/I has the form J/I, for some ideal satisfying $I \subseteq J \subseteq R$.

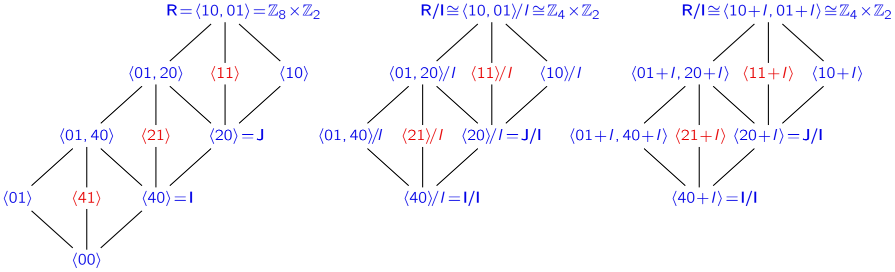


Big idea

This is just like the correspondence theorem for groups, but it also "preserves colors."

The correspondence theorem: subrings of quotients

"*The ideals of a quotient R/I are just the quotients of the ideals that contain I.*"



"*shoes out of the box*"

30	70	31	71
10	50	11	51
20	60	21	61
00	40	01	41

$J = \langle 20 \rangle \leq R$

"*shoeboxes; lids off*"

30	70	31	71
10	50	11	51
20	60	21	61
00	40	01	41

$\langle 20 \rangle / I \leq R/I$

"*shoeboxes; lids on*"

$30 + I$	$31 + I$
$10 + I$	$11 + I$
$20 + I$	$21 + I$
I	$01 + I$

$\langle 20 + I \rangle \leq R/I$

The correspondence theorem: subrings of quotients

Correspondence theorem (informally)

There is a bijection between subrings of R/I and subrings of R that contain I.

"Everything that we want to be true" about the subring lattice of R/I is inherited from the subring lattice of R.

Most of these can be summarized as:

"The __________ of the quotient is just the quotient of the __________"

Correspondence theorem (formally)

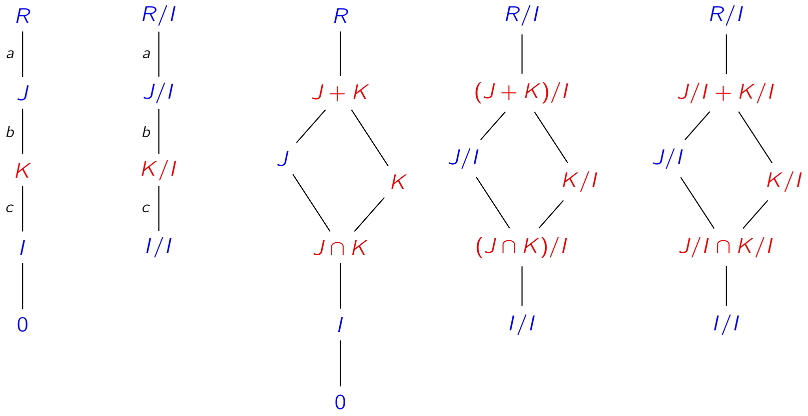
Let $I \leq J \leq R$ and $I \leq K \leq R$ be chains of subrings and $I \trianglelefteq R$. Then

1. Subrings of the quotient R/I are quotients of subrings that contain I.
2. $J/I \trianglelefteq R/I$ if and only if $J \trianglelefteq R$
3. $[R/I : J/I] = [R : J]$
4. $J/I \cap K/I = (J \cap K)/I$
5. $J/I + K/I = (J + K)/I$

The correspondence theorem: subring structure of quotients

All parts of the correspondence theorem have nice subring lattice interpretations.

We've already interpreted the first part. Here's what the next four parts say.



The fraction theorem: quotients of quotients

The correspondence theorem characterizes the subring structure of the quotient R/I.

Every subring of R/I is of the form J/I, where $I \leq J \leq R$.

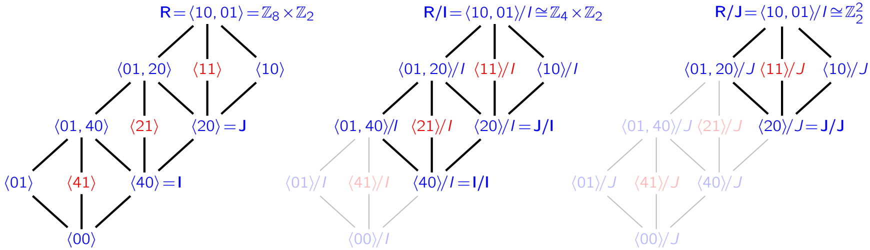
Moreover, if $J \trianglelefteq R$ is an ideal, then $J/I \trianglelefteq R/I$. In this case, we can ask:

"*What is the quotient ring $(R/I)/(J/I)$ isomorphic to?*"

Fraction theorem

Given a chain $I \leq J \leq R$ of ideals of R,

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

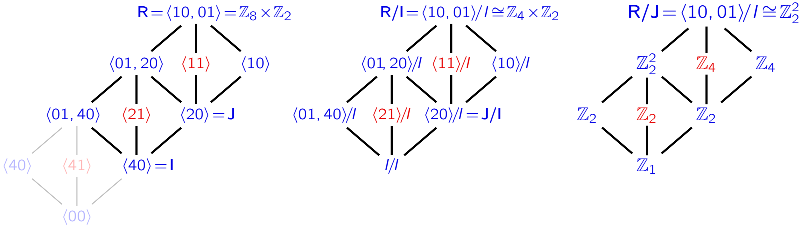


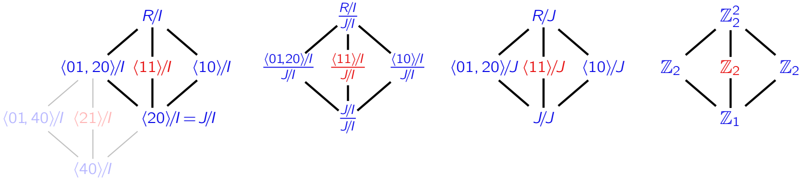
The fraction theorem: quotients of quotients

Fraction theorem

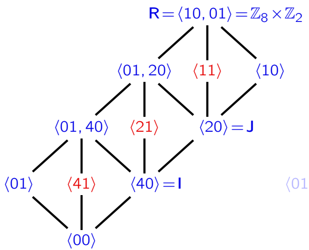
Given a chain $I \leq J \leq R$ of ideals of R,

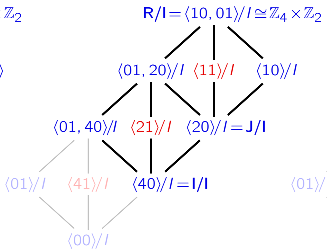
$$(R/I)/(J/I) \cong R/J.$$

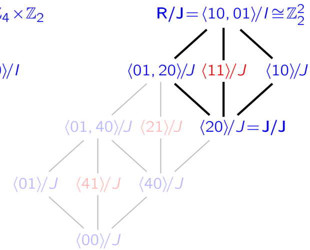


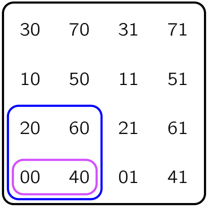


The fraction theorem: quotients of quotients

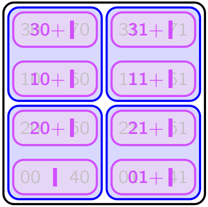






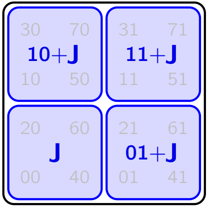


$I \leq J \leq R$



R/I consists of 8 cosets

$J/I = \{I,\ 20+I\}$



R/J consists of 4 cosets

$(R/I)/(J/I) \cong R/J \cong \mathbb{Z}_2^2$

The fraction theorem: quotients of quotients

For another visualization, consider $R = \mathbb{Z}_6 \times \mathbb{Z}_4$ and write elements as strings.

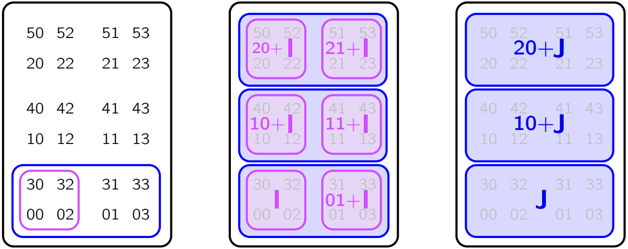
Consider the ideals $J = \langle 30, 02 \rangle \cong \mathbb{Z}_2^2$ and $I = \langle 30, 01 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

Notice that $I \leq J \leq R$, and $I = J \cup (01+J)$, and

$$R/I = \big\{I,\ 01+I,\ 10+I,\ 11+I,\ 20+I,\ 21+I\big\}, \qquad J/I = \{I,\ 01+I\}$$

$$R/J = \Big\{I \cup (01+I),\ (10+I) \cup (11+I),\ (20+I) \cup (21+I)\Big\}$$

$$(R/I)/(J/I) = \Big\{\{I,\ 01+I\},\ \{10+I,\ 11+I\},\ \{20+I,\ 21+I\}\Big\}.$$

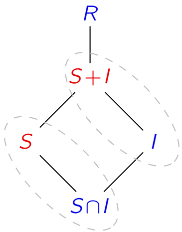


$I \leq J \leq R$

R/I consists of 6 cosets
$J/I = \big\{I,\ 01+I\big\}$

R/J consists of 3 cosets
$(R/I)/(J/I) \cong R/J$

The diamond theorem: duality of subquotients



Diamond theorem

Suppose S is a subring and I an ideal of R. Then

(i) The intersection $S \cap I$ is an ideal of S.

(ii) The following quotient rings are isomorphic:

$$(S+I)/I \cong S/(S \cap I)\,.$$

Proof (sketch)

(i) Showing $S \cap I$ is an ideal of S is straightforward (exercise).

(ii) We already know that $(S+I)/I \cong S/(S \cap I)$ as additive groups.

Recall that we proved this by applying the FHT to the (group) homomorphism

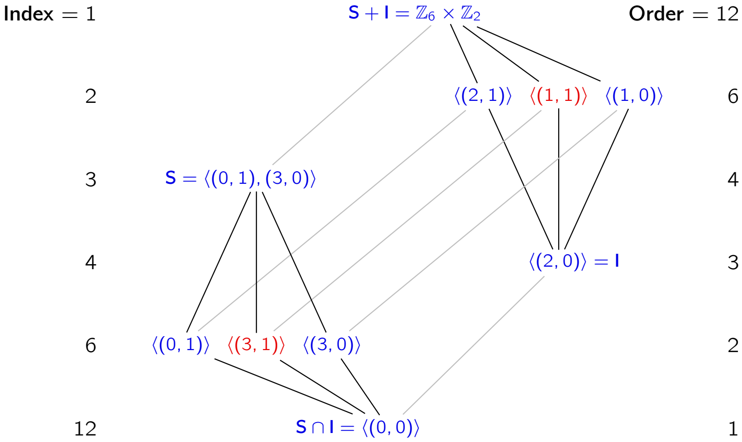
$$\phi\colon S \longrightarrow (S+I)/I, \qquad \phi\colon s \longmapsto s+I.$$

It remains to show that ϕ is a ring homomorphism, i.e., $\phi(s_1 s_2) = \phi(s_1)\phi(s_2)$. □

The diamond theorem: duality of subquotients

Like for groups, the diamond theorem guarantees an inherent "duality" in subring lattices.

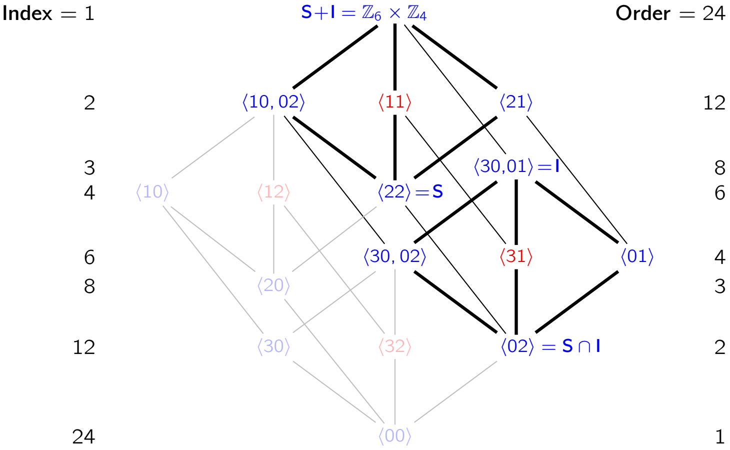
For rings, it also "preserves the colors" – subgroup, subring, and ideal structure.



The diamond theorem: duality of subquotients

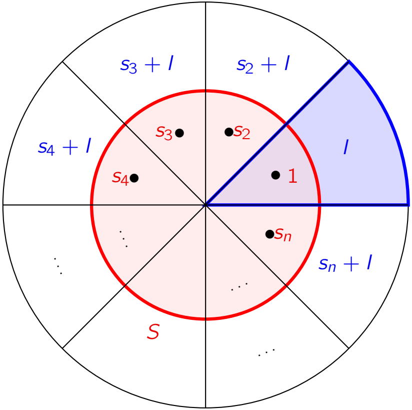
Like for groups, the diamond theorem guarantees an inherent "duality" in subring lattices.

For rings, it also "preserves the colors" – subgroup, subring, and ideal structure.



The diamond theorem illustrated by a "pizza diagram"

The following analogy is due to Douglas Hofstadter:



$S + I =$ large pizza

$S =$ small pizza

$I =$ large pizza slice

$S \cap I =$ small pizza slice

$(S + I)/I = \{\text{large pizza slices}\}$

$S/(S \cap I) = \{\text{small pizza slices}\}$

Diamond theorem: $(S + I)/I \cong S/(S \cap I)$

Theorem (exercise)

Every homomorphism $\phi \colon R \to S$ can be factored as a quotient and embedding: