Math 332 Winter 2023, Lecture 9: Rings

website: `https://www.cip.ifi.lmu.de/~grinberg/t/23wa`

1. Rings and ideals (cont'd)

1.9. Quotient rings (cont'd)

1.9.3. More examples of quotient rings

Recall: If R is a ring, and I is an ideal of R, then R/I is the **quotient ring** of R by I.

Its elements are the **cosets** $r+I$, also called **residue classes** and denoted by $\overline{r}$ (if I is clear from the context).

A residue class $\overline{r} = r + I$ is (formally speaking) the set of all $r+i$ where i ranges over I.

Two residue classes $\overline{r}$ and $\overline{s}$ are identical if and only if $r - s \in I$. (Thus, passing from R to R/I amounts to "equating" any two elements that differ only by an element of I.)

Addition and multiplication of residue classes are defined "by representatives":

$$\overline{a} + \overline{b} = \overline{a+b};$$
$$\overline{a} \cdot \overline{b} = \overline{ab} \qquad \text{for all } a, b \in R.$$

The most basic example of a quotient ring is $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$. For instance, if $n = 2$, then $\mathbb{Z}/n = \mathbb{Z}/2$ has only two elements: $\overline{0} = \{\text{all even integers}\}$ and $\overline{1} = \{\text{all odd integers}\}$, and the rule for addition in $\mathbb{Z}/2$ says (e.g.) that $\overline{1} + \overline{1} = \overline{1+1} = \overline{2} = \overline{0}$ (or, in colloquial terms, "odd + odd = even").

In Lecture 8, we saw a few examples of quotient rings. Here are two more:

- As we recall, if R is a ring and $n \in \mathbb{N}$ an integer, then

$$\begin{aligned} R^{n \leq n} &= \{\text{all upper-triangular } n \times n\text{-matrices with entries in } R\} \\ &= \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ & a_{2,2} & \cdots & a_{2,n} \\ & & \ddots & \vdots \\ & & & a_{n,n} \end{pmatrix} \mid a_{i,j} \in R \text{ for all } i \leq j \right\} \end{aligned}$$

  (where empty spaces stand for entries that are 0) is a ring.

  Let us consider the special case $R = \mathbb{Q}$ and $n = 3$ for simplicity (although everything we are doing can be generalized to arbitrary R and n). Thus,

$$R^{n \leq n} = \mathbb{Q}^{3 \leq 3} = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mid a, b, c, d, e, f \in \mathbb{Q} \right\}.$$

I claim that the subset

$$\begin{aligned}\mathbb{Q}^{3<3} &:= \{\text{all strictly upper-triangular } 3\times 3\text{-matrices with entries in } \mathbb{Q}\} \\ &= \left\{ \begin{pmatrix} 0 & b & c \\ 0 & 0 & e \\ 0 & 0 & 0 \end{pmatrix} \ \mid\ b,c,e \in \mathbb{Q} \right\}\end{aligned}$$

is an ideal of $\mathbb{Q}^{3\leq 3}$. To prove this, we need to show that it satisfies the three ideal axioms. The first and the third axioms are obvious (e.g., a sum of two strictly upper-triangular matrices is again strictly upper-triangular). To prove the second ideal axiom, we need to show that if $A \in \mathbb{Q}^{3<3}$ is strictly upper-triangular and $B \in \mathbb{Q}^{3\leq 3}$ is just upper-triangular, then AB and BA are strictly upper-triangular. This can just be checked by hand: Both products

$$\begin{pmatrix} 0 & x & y \\ 0 & 0 & z \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} = \begin{pmatrix} 0 & dx & ex+fy \\ 0 & 0 & fz \\ 0 & 0 & 0 \end{pmatrix} \qquad \text{and}$$

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \begin{pmatrix} 0 & x & y \\ 0 & 0 & z \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ax & ay+bz \\ 0 & 0 & dz \\ 0 & 0 & 0 \end{pmatrix}$$

are strictly upper-triangular.[1] More generally, when you multiply two upper-triangular matrices, the diagonal entries get multiplied entrywise: e.g.,

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \begin{pmatrix} a' & b' & c' \\ 0 & d' & e' \\ 0 & 0 & f' \end{pmatrix} = \begin{pmatrix} aa' & bd'+ab' & be'+cf'+ac' \\ 0 & dd' & de'+ef' \\ 0 & 0 & ff' \end{pmatrix}.$$

Thus, if one of the two matrices has a zero diagonal, then the product will also have a zero diagonal. So we see again that $\mathbb{Q}^{3<3}$ is an ideal of $\mathbb{Q}^{3\leq 3}$.

What is the quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$? Any element of this quotient ring has the form

$$\overline{A} = A + \mathbb{Q}^{3<3} \qquad \text{for some } A \in \mathbb{Q}^{3\leq 3}.$$

Such a residue class $\overline{A}$ is a coset of $\mathbb{Q}^{3<3}$, so it consists of all matrices that can be obtained from A by adding a strictly upper-triangular matrix. For

[1]The analogous claim holds for arbitrary R and n (not just for $R = \mathbb{Q}$ and $n = 3$), and can be proved using the definition of a matrix product.

example, if $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}$, then

$$\begin{aligned}
\overline{A} = A + \mathbb{Q}^{3<3} &= \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix} + \left\{ \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \mid a,b,c \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix} + \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \mid a,b,c \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} 1 & 2+a & 3+b \\ 0 & 4 & 5+c \\ 0 & 0 & 6 \end{pmatrix} \mid a,b,c \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 4 & z \\ 0 & 0 & 6 \end{pmatrix} \mid x,y,z \in \mathbb{Q} \right\},
\end{aligned}$$

We shall thus denote this coset by

$$\begin{pmatrix} 1 & \mathbb{Q} & \mathbb{Q} \\ 0 & 4 & \mathbb{Q} \\ 0 & 0 & 6 \end{pmatrix},$$

where the $\mathbb{Q}$'s mean "you can put an arbitrary element of $\mathbb{Q}$ here". So you can think of $\overline{A}$ as a "matrix" in which the three entries above the diagonal are undetermined. (Formally, this is a set of matrices.)

The rules for adding and multiplying such "partly determined matrices" are just as you would expect: e.g.,

$$\begin{pmatrix} a & \mathbb{Q} & \mathbb{Q} \\ 0 & b & \mathbb{Q} \\ 0 & 0 & c \end{pmatrix} \begin{pmatrix} d & \mathbb{Q} & \mathbb{Q} \\ 0 & e & \mathbb{Q} \\ 0 & 0 & f \end{pmatrix} = \begin{pmatrix} ad & \mathbb{Q} & \mathbb{Q} \\ 0 & be & \mathbb{Q} \\ 0 & 0 & cf \end{pmatrix}.$$

You might observe that the undetermined $\mathbb{Q}$-entries are just "acting like zeroes" here: The formula we just saw looks exactly like the formula

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \begin{pmatrix} d & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & f \end{pmatrix} = \begin{pmatrix} ad & 0 & 0 \\ 0 & be & 0 \\ 0 & 0 & cf \end{pmatrix}$$

for multiplying diagonal matrices, except that we have $\mathbb{Q}$'s instead of 0's above the diagonal. The same holds for addition instead of multiplication. Thus, the residue classes in $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$ are behaving like diagonal matrices. In essence, we are saying that

$$\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3} \cong \mathbb{Q}^{3=3},$$

where $\mathbb{Q}^{3=3}$ is the ring of diagonal 3×3-matrices (yes, they do form a ring – to be precise, a subring of $\mathbb{Q}^{3\times 3}$). To be more specific: The map

$$\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3} \to \mathbb{Q}^{3=3},$$
$$\overline{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}} \mapsto \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix}$$

is a ring isomorphism. (To prove this, you need to show that this map is well-defined, is a ring morphism, and is invertible.)

This means that we have been wasting time defining the quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$. After all, we want to find something new, not to recover an isomorphic copy of a known ring like $\mathbb{Q}^{3=3}$!

- Let us try again. Again consider the ring $\mathbb{Q}^{3\leq 3}$ of upper-triangular 3×3-matrices over $\mathbb{Q}$. Now, consider the set

$$\mathbb{Q}^{3<<3} := \left\{ \begin{pmatrix} 0 & 0 & y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mid y \in \mathbb{Q} \right\}.$$

This set $\mathbb{Q}^{3<<3}$ is again an ideal of $\mathbb{Q}^{3\leq 3}$, because

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \begin{pmatrix} 0 & 0 & y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & ay \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \text{and}$$
$$\begin{pmatrix} 0 & 0 & y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} = \begin{pmatrix} 0 & 0 & fy \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

(the other ideal axioms are again easy).

What is the quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3}$? A residue class $\overline{A} = A + \mathbb{Q}^{3<<3}$

in this quotient ring looks as follows:

$$\begin{aligned}
\overline{A} &= \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} + \mathbb{Q}^{3<<3} \\
&= \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} + \left\{ \begin{pmatrix} 0 & 0 & y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mid y \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} + \begin{pmatrix} 0 & 0 & y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mid y \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} a & b & c+y \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mid y \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} a & b & z \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mid z \in \mathbb{Q} \right\} \\
&= \begin{pmatrix} a & b & \mathbb{Q} \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}.
\end{aligned}$$

This is again a matrix "with an undetermined entry", but this time it has 8 determined entries (including the zeroes under the diagonal) and only one undetermined entry. In particular, it is no longer "just a diagonal matrix in disguise". Here is how we multiply such "partly determined matrices":

$$\begin{pmatrix} a & b & \mathbb{Q} \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \cdot \begin{pmatrix} a' & b' & \mathbb{Q} \\ 0 & d' & e' \\ 0 & 0 & f' \end{pmatrix} = \begin{pmatrix} aa' & bd' + ab' & \mathbb{Q} \\ 0 & dd' & f'e + de' \\ 0 & 0 & ff' \end{pmatrix}.$$

For comparison, if we had zeroes instead of undetermined $\mathbb{Q}$-entries, multiplication would look as follows:

$$\begin{pmatrix} a & b & 0 \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \cdot \begin{pmatrix} a' & b' & 0 \\ 0 & d' & e' \\ 0 & 0 & f' \end{pmatrix} = \begin{pmatrix} aa' & bd' + ab' & be' \\ 0 & dd' & f'e + de' \\ 0 & 0 & ff' \end{pmatrix}.$$

Note the be' entry (which, in general, is not 0) in the top right cell! Thus, the set of all matrices of the form $\begin{pmatrix} * & * & 0 \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix}$ (where a $*$ stands for an arbitrary entry) is not a subring of $\mathbb{Q}^{3\leq 3}$. Thus, unlike in our previous example, our "partly determined matrices" cannot be emulated by regular matrices by putting 0's in the positions of the undetermined $\mathbb{Q}$-entries. Thus, $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3}$ is not isomorphic to a subring of $\mathbb{Q}^{3\leq 3}$ (at least not in an obvious way). So we have obtained a genuinely new ring this time.

1.9.4. The canonical projection

Theorem 1.8.4 in Lecture 7 says that the kernel of any ring morphism is an ideal of its domain. Now we will prove the converse: Any ideal is a kernel. Better yet:

> **Theorem 1.9.5.** Let R be a ring. Let I be an ideal of R. Consider the map
>
> $$\begin{aligned} \pi : R &\to R/I, \\ r &\mapsto r + I = \overline{r}. \end{aligned}$$
>
> This map π is a surjective ring morphism with kernel I.

This morphism π is called the **canonical projection** from R onto R/I.

Proof of Theorem 1.9.5. To prove that π is a ring morphism, we need to check that π respects addition, multiplication, zero and unity. This is all straightforward. For example, π respects multiplication because all $a, b \in R$ satisfy

$$\begin{aligned} \underbrace{\pi(a)}_{=\overline{a}} \cdot \underbrace{\pi(b)}_{=\overline{b}} &= \overline{a} \cdot \overline{b} = \overline{ab} && \text{(by the definition of multiplication on } R/I\text{)} \\ &= \pi(ab). \end{aligned}$$

Thus, π is a ring morphism.

Why is π surjective? Because (by definition) each element of R/I is a residue class, i.e., has the form $\overline{r}$ for some $r \in R$.

Finally, π has kernel I, since

$$\begin{aligned} \operatorname{Ker} \pi &= \{r \in R \mid \pi(r) = 0_{R/I}\} && \text{(by the definition of a kernel)} \\ &= \left\{r \in R \mid \pi(r) = \overline{0}\right\} && \left(\text{since } 0_{R/I} = \overline{0}\right) \\ &= \left\{r \in R \mid \overline{r} = \overline{0}\right\} && \left(\text{since } \pi(r) = \overline{r} \text{ by definition of } \pi\right) \\ &= \{r \in R \mid r - 0 \in I\} \\ &= \{r \in R \mid r \in I\} = I. \end{aligned}$$

□

For example, if we take $R = \mathbb{Z}$ and $I = 2\mathbb{Z}$ in Theorem 1.9.5, then the canonical projection π is the map

$$\begin{aligned} \pi : \mathbb{Z} &\to \mathbb{Z}/2, \\ r &\mapsto r + 2\mathbb{Z} = \overline{r}. \end{aligned}$$

This map π sends each even integer to $\overline{0}$ and each odd integer to $\overline{1}$. In other words, π assigns to each integer its parity (as an element of $\mathbb{Z}/2$).