Math 332 Winter 2023, Lecture 8: Rings

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

1. Rings and ideals (cont'd)

1.9. Quotient rings (cont'd)

1.9.2. Quotient rings (cont'd)

Last time, we made the following definition and stated the theorem that comes after it:

Definition 1.9.3. Let I be an ideal of a ring R. Thus, I is a subgroup of the additive group $(R, +, 0)$, hence a normal subgroup (since $(R, +, 0)$ is abelian). Thus, the quotient group R/I is a well-defined abelian group. Its elements are the cosets $r + I$ of I in R. These cosets are called the **residue classes** modulo I. A coset $r + I$ is also denoted by $\overline{r}$ or $[r]$ or $[r]_I$ or $r \bmod I$. (We will only use the notations $\overline{r}$ and $r + I$.)

Note that the addition on R/I is given by

$$(a + I) + (b + I) = (a + b) + I \qquad \text{for all } a, b \in R. \tag{1}$$

We now define a multiplication operation on R/I by setting

$$(a + I)(b + I) = ab + I \qquad \text{for all } a, b \in R. \tag{2}$$

(See below for a proof that this is well-defined.)

The set R/I, equipped with the addition and the multiplication we just defined, and with the elements $0 + I$ and $1 + I$ playing the roles of zero and unity, is a ring (as we will soon see). This ring is called the **quotient ring** of R by the ideal I, and is denoted by R/I. It is pronounced "R **modulo** I".

Theorem 1.9.4. Let R and I be as in this definition. Then, the multiplication on R/I is well-defined, and R/I becomes a ring when endowed with the operations we just introduced.

Note that the rules (1) and (2), by which we defined addition and multiplication on R/I, can be rewritten as

$$\overline{a} + \overline{b} = \overline{a + b} \qquad \text{for all } a, b \in R \tag{3}$$

and

$$\overline{a} \cdot \overline{b} = \overline{ab} \qquad \text{for all } a, b \in R. \tag{4}$$

We will prove Theorem 1.9.4 later today. First, however, a few examples:

- Let $n \in \mathbb{Z}$. Then, the set $n\mathbb{Z} = \{\text{all multiples of } n\}$ is an ideal of $\mathbb{Z}$ (a principal ideal, in fact). The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is exactly the ring $\mathbb{Z}/n$ of residue classes modulo n that we introduced a while ago. In fact, the above definition of R/I is just the natural generalization of the definition of the ring $\mathbb{Z}/n$, where we replaced integers by elements of R and multiples of n by elements of I.

- Two stupid general examples:

  Recall that every ring R has at least the ideals $\{0_R\}$ and R. What are the respective quotient rings?

  - The quotient ring $R/\{0_R\}$ is isomorphic to R. Indeed, each residue class modulo $\{0_R\}$ has the form $r + \{0_R\} = \{r\}$, which is a 1-element set. Thus, the elements of $R/\{0_R\}$ are just the elements of R "stuck in set braces", with the same rules for adding and multiplying as in R (that is, $\{a\} + \{b\} = \{a+b\}$ and $\{a\} \cdot \{b\} = \{ab\}$).
  - The quotient ring R/R is trivial. Indeed, there is only one residue class modulo R, and this class contains all elements of R. (In fact, for any $r \in R$, the corresponding residue class $r + R$ is R itself.)

  These are the most boring quotient rings you can imagine. Interesting things happen when the ideal I is "between" $\{0_R\}$ and R.

- Let R be the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ of Gaussian integers. Consider its principal ideal

$$\begin{aligned} 3R &= \{3r \mid r \in R\} \\ &= \{3r \mid r \in \mathbb{Z}[i]\} \\ &= \{3a + 3bi \mid a, b \in \mathbb{Z}\} \\ &= \{c + di \mid c, d \in \mathbb{Z} \text{ are multiples of } 3\}. \end{aligned}$$

  What is the quotient ring $R/(3R)$? The elements of this ring have the form

$$\overline{a + bi} \qquad \text{with } a, b \in \{0, 1, 2\}$$

  (do not confuse the line over the $a + bi$ with the identical-looking notation for "complex conjugate"; we are not using complex conjugates anywhere in this example). In fact, any Gaussian integer can be reduced to a Gaussian integer of the form $a + bi$ with $a, b \in \{0, 1, 2\}$ by subtracting an appropriate Gaussian-integer multiple of 3 (because we can subtract a multiple of 3 to turn its real part into one of $0, 1, 2$, and then subtract a multiple of $3i$ to turn its imaginary part into one of $0, 1, 2$). In other words,

$$R/(3R) = \left\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{i},\ \overline{1+i},\ \overline{2+i},\ \overline{2i},\ \overline{1+2i},\ \overline{2+2i}\right\}.$$

It is easy to see that this is a 9-element ring (i.e., the residue classes $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{i}$, $\overline{1+i}$, $\overline{2+i}$, $\overline{2i}$, $\overline{1+2i}$, $\overline{2+2i}$ are distinct), and a field (i.e., all the nonzero residue classes are invertible). So we have found a little finite field with 9 elements.

Let us do some computations in this field: We have

$$\overline{2+i}+\overline{2+2i}=\overline{(2+i)+(2+2i)}=\overline{4+3i}=\overline{1}$$

since $(4+3i)-1=3(1+i)\in 3R$. Also,

$$\overline{2+i}\cdot\overline{2+2i}=\overline{(2+i)(2+2i)}=\overline{2\cdot 2+2\cdot 2i+i\cdot 2+i\cdot 2i}$$
$$=\overline{4+4i+2i-2}=\overline{2+6i}=\overline{2},$$

since $(2+6i)-2=3\cdot 2i\in 3R$. Similarly,

$$\overline{2+i}\cdot\overline{1+i}=\overline{1},$$

which shows that the elements $\overline{2+i}$ and $\overline{1+i}$ are inverse to each other in $R/(3R)$.

For the curious: If we replace 3 by any other positive integer n, then $R/(nR)$ will be a finite ring with n^2 elements. Depending on the value of n, it will or won't be a field. For instance, we found that it is a field for $n=3$. However, it is not a field for $n=5$, because in $R/(5R)$, we have

$$\overline{1+2i}\cdot\overline{1-2i}=\overline{(1+2i)(1-2i)}=\overline{1+4}=\overline{5}=\overline{0}.$$

We will learn more about when $R/(nR)$ is a field later on.

- Again take $R=\mathbb{Z}[i]$, but now consider the quotient ring $R/((1+i)R)$. How many elements does it have? The answer is 2, but this is not that obvious any more, because how can we tell which Gaussian integers belong to $(1+i)R$ (that is, are Gaussian-integer multiples of $1+i$) ?

  Here is one way to prove that $R/((1+i)R)$ has 2 elements (and to find these elements):

  - Observe that $2\in(1+i)R$ (because $2=(1+i)(1-i)$). Thus, every Gaussian integer can be reduced to a Gaussian integer of the form $a+bi$ with $a,b\in\{0,1\}$ by adding an element of $(1+i)R$.
  - Thus, $R/((1+i)R)=\{\overline{0},\ \overline{1},\ \overline{i},\ \overline{1+i}\}$.
  - Furthermore, $\overline{0}=\overline{1+i}$ and $\overline{1}=\overline{i}$ (why?).
  - Thus, $R/((1+i)R)=\{\overline{0},\ \overline{1}\}$ (why?).
  - Finally, we have $\overline{0}\neq\overline{1}$, since $0-1$ is not a multiple of $1+i$ (because $\dfrac{0-1}{1+i}=\dfrac{-1}{1+i}=\dfrac{-1(1-i)}{(1+i)(1-i)}=\dfrac{-1+i}{2}=\dfrac{-1}{2}+\dfrac{1}{2}i$ is not a Gaussian integer).

- Consequently, $R/\left((1+i)\,R\right)$ consists of the two distinct elements $\overline{0}$ and $\overline{1}$.

Can we analyze $R/\left((7+9i)\,R\right)$ likewise? What about $R/\left((a+bi)\,R\right)$ for general a and b ? This will be a ring of size a^2+b^2 (unless $a=b=0$), but we don't quite have the tools to prove this yet.

See the text for a few more examples (some of which will be on homework set #3).

Let us now make good on our debts and prove Theorem 1.9.4:

Proof of Theorem 1.9.4. We must prove that the operations $+$ and $\cdot$ on R/I are well-defined, and that R/I is a ring when equipped with these operations.

The latter is very easy: All the ring axioms are inherited from R. For example, to see that $\cdot$ on R/I is associative, we must show that $\overline{a}\cdot\left(\overline{b}\cdot\overline{c}\right)=\left(\overline{a}\cdot\overline{b}\right)\cdot\overline{c}$ for all $a,b,c\in R$; but this is clear since the LHS is $\overline{a\,(bc)}$ by definition and the RHS is $\overline{(ab)\,c}$ by definition and since associativity of multiplication in R yields $a\,(bc)=(ab)\,c$.

The harder part is the first part: We must show that $+$ and $\cdot$ on R/I are well-defined. For $+$, this has already been done in group theory (it is part of what it means for the quotient **group** R/I to be well-defined). Thus, we only need to do it for $\cdot$.

Well-definedness for $\cdot$ means that the product $\overline{a}\cdot\overline{b}$ of two residue classes $\overline{a}=a+I$ and $\overline{b}=b+I$ depends **only on these residue classes** and not on the elements $a,b\in R$ themselves. In other words, it means that if x and y are two residue classes modulo I, and if we compute their product xy using the formula (4) by writing x as $\overline{a}$ and y as $\overline{b}$ for some $a,b\in R$, then the exact choices of a and b do not affect the resulting value $xy=\overline{ab}$.

To prove this, we must therefore show the following: If one and the same residue class in R/I can be written both as $\overline{a}$ and as $\overline{a'}$, and if one and the same residue class in R/I can be written both as $\overline{b}$ and as $\overline{b'}$, then $\overline{ab}=\overline{a'b'}$.

In other words, we must show the following: If four elements $a,b,a',b'\in R$ satisfy $\overline{a}=\overline{a'}$ and $\overline{b}=\overline{b'}$, then $\overline{ab}=\overline{a'b'}$.

This is the ring-theoretical generalization of the well-known fact that if five integers $a,b,a',b',n\in\mathbb{Z}$ satisfy $a\equiv a' \bmod n$ and $b\equiv b' \bmod n$, then $ab\equiv a'b' \bmod n$. As we recall, this classical fact can be proved by rewriting $a\equiv a' \bmod n$ as $a=a'+nx$ for some integer x, and likewise rewriting $b\equiv b' \bmod n$ as $b=b'+ny$ for some integer y, and then multiplying these two equalities to find

$$ab=\left(a'+nx\right)\left(b'+ny\right)=a'b'+\underbrace{a'ny+nxb'+nxny}_{\text{divisible by } n}\equiv a'b' \bmod n.$$

The proof of the ring-theoretical generalization is not much different: Let $a,b,a',b'\in R$ satisfy $\overline{a}=\overline{a'}$ and $\overline{b}=\overline{b'}$. Then, from $\overline{a}=\overline{a'}$, we obtain $a-a'\in I$.

In other words, $a - a' = i$ for some $i \in I$. Similarly, $b - b' = j$ for some $j \in I$. Consider these i and j. From $a - a' = i$, we obtain $a = a' + i$. Similarly, $b = b' + j$. Multiplying the latter two equalities, we obtain

$$ab = \left(a' + i\right) \left(b' + j\right) = a'b' + a'j + ib' + ij.$$

Hence, we can conclude that $\overline{ab} = \overline{a'b'}$ if we can show that $a'j + ib' + ij \in I$. But this follows from the ideal axioms, since i and j belong to I. (In more detail: The second ideal axiom yields $a'j \in I$ and $ib' \in I$ and $ij \in I$; then, the first ideal axiom yields $a'j + ib' + ij \in I$.)

Thus, we have proved that $\overline{ab} = \overline{a'b'}$ (since $ab = a'b' + \underbrace{a'j + ib' + ij}_{\in I}$ shows that ab and $a'b'$ belong to the same coset of I in R). This concludes the proof that the operation $\cdot$ on R/I is well-defined. As we said, this also completes our proof of Theorem 1.9.4. $\square$