Lecture 12

Computations, and polynomials over fields

12.1 $\mathbb{Z}/n\mathbb{Z}$

Fix an integer n. Let's dive a bit deeper into $\mathbb{Z}/n\mathbb{Z}$.

12.1.1 Clocks

As you know, $\mathbb{Z}/n\mathbb{Z}$ is defined as a quotient ring. Writing $[i]$ for the equivalence class of $i \in \mathbb{Z}$, we have seen that $\mathbb{Z}/n\mathbb{Z}$ consists of n elements:

$$[0], \qquad [1], \qquad \ldots, \qquad [n-1].$$

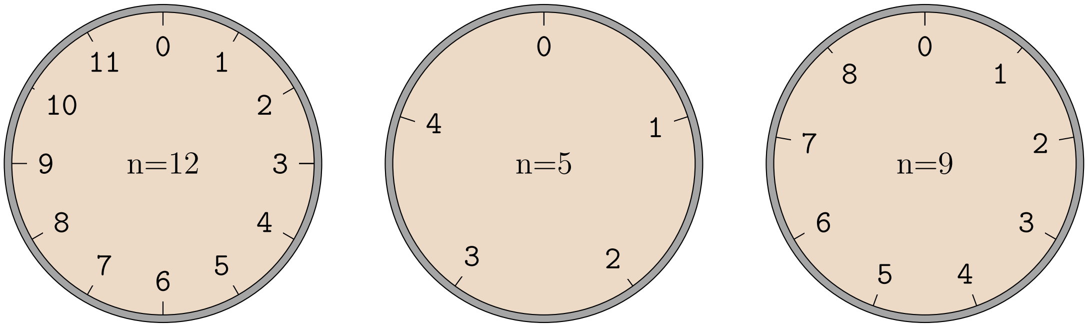
Explicitly, the equivalence class $[i]$ is a set consisting of elements as follows:

$$[i] = \{\ldots, i-3n, i-2n, i-n, i, i+n, i+2n, i+3n, \ldots\}.$$

We see a bijection between the set $\mathbb{Z}/n\mathbb{Z}$ and the set $\{0, 1, \ldots, n-1\}$ as follows:

$$\{0, 1, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z} \qquad i \mapsto [i].$$

Using this bijection, we can also think about $\mathbb{Z}/n\mathbb{Z}$'s elements as consisting of hours on an n-hour clock. Here are some examples for various n:



You are probably most familiar with the example of $n = 12$. If it is 8 o'clock now, then 9 hours from now, it will be 5 o'clock. This is reflected in the following equation taking place in $\mathbb{Z}/12\mathbb{Z}$:

$$[8] + [9] = [5] \in \mathbb{Z}/12\mathbb{Z}.$$

If instead we were to use a nine-hour clock, then the above computation would be

$$[8] + [9] = [8] \in \mathbb{Z}/9\mathbb{Z}.$$

Multiplication has a similar interpretation. Let's say again that you're on a twelve-hour clock (the kind we're used to). If you begin at zero o-clock, and move 8 times in 2-hour increments, you move a total of 16 hours, meaning you end up at 4 o'clock. This would be written

$$[8] \times [2] = [16] = [4] \in \mathbb{Z}/12\mathbb{Z}.$$

If we were on a nine-hour clock, we would find

$$[8] \times [2] = [16] = [7] \in \mathbb{Z}/9\mathbb{Z}.$$

12.1.2 Addition tables

It's not terribly exciting, but we can organize the values of addition into tables. A number in the a column and the b row is the value of $a + b$.

In the tables below, we are using the bijection from before, so 3 really represents the element [3] in $\mathbb{Z}/n\mathbb{Z}$. They are addition tables for $n = 2, 4, 5$:

+	0	1
0	0	1
1	1	0

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

You should check them for their accuracy.

The diagonal entries represent elements of the form $x + x$, or what we would write as $2x$. In $\mathbb{Z}/4\mathbb{Z}$, only the elements 0 and 2 appear as $x + x$. In $\mathbb{Z}/5\mathbb{Z}$, every element appears along the diagonal. This means that for any $a \in \mathbb{Z}/5\mathbb{Z}$, the equation $2x = a$ can be solved in $\mathbb{Z}/5\mathbb{Z}$.

12.1.3 Multiplication tables

We can likewise create multiplication tables. Here, the entry in row b and column a is the element ab in $\mathbb{Z}/n\mathbb{Z}$. Here are multiplication tables for $n = 2, 4, 5$:

+	0	1
0	0	0
1	0	1

+	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

+	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The diagonal entries represent the square numbers in your ring. For example, in $\mathbb{Z}/4\mathbb{Z}$, the only square numbers are 0 and 1. We have interesting equations like $2^2 = 0$ and $3^2 = 1$.

In $\mathbb{Z}/5\mathbb{Z}$, we see that the only square numbers are 0, 1, and 4.

You can also check whether an element a admits a multiplicative inverse by seeing if there is a 1 in the row (or column) labeled by a. For example, for $n = 4$, we see that the 3 row has a 1 in it, so 3 has a multiplicative inverse. In fact, 3 is its own inverse, as $3 \times 3 = 1$ in $\mathbb{Z}/4\mathbb{Z}$.

In $\mathbb{Z}/5\mathbb{Z}$, every non-zero element has a multiplicative inverse. We can read from the table that $2 \times 3 = 1$ and $4 \times 4 = 1$ (so 4 is its own inverse).

Remark 12.1.1. Note that $1 + (n - 1) = 0$ in $\mathbb{Z}/n\mathbb{Z}$, so the element $(n - 1)$ (also known as $[n - 1]$) is the additive inverse to 1. In other words, one can also express $n - 1$ as simply -1. Then, as you've proven in a previous exercise, $(-1)^2 = 1$, so $n-1$ is always its own multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$.

12.2 Dividing polynomials

Not everybody learns about dividing polynomials, so I'd like to review it.

First, what do I mean by polynomial division? Well, recall that in division of whole numbers, we have the following result:

Proposition 12.2.1. Let a and b be positive integers. Then there exists unique positive integers q, r so that

$$a = qb + r$$

and for which $0 \leq r < b$. Moreover, q and r are unique. (So if $a = q'b + r'$ with $r' < b$, then we must have that $q = q'$ and $r = r'$.)

We often say that r is the remainder of dividing a by b.

Example 12.2.2. $103 = 14 \times 7 + 5$, so 103 divided by 7 is 14 with remainder 5. In this case, $a = 103$, $b = 7$ and the quotient $q = 14$ with remainder $r = 5$.

Incredibly important is the idea that the remainder is something with some bound on its size: r is between 0 and $b - 1$, inclusive.

It's harder to say what the "size" of a polynomial is, but we've seen the utility of an invariant called "degree" of a polynomial. The following proposition shows that degree does, in many ways, behave like size:

Theorem 12.2.3. Let R be a field, and fix two polynomials $a, b \in R[x]$. Then there exist polynomials $q, r \in R[x]$ for which

$$a = qb + r$$

and where $\deg(r) < \deg(b)$. Moreover, q and r are unique. (So if $a = q'b + r'$ with $\deg r' < \deg b$, then we must have that $q = q'$ and $r = r'$.)

In other words, we can always try to divide a polynomial $a(x)$ by another polynomial $b(x)$, and even if b doesn't "fit" perfectly into a, we can guarantee a remainder whose *degree* is strictly smaller than the degree of b.

Remark 12.2.4. The assumption that R is a field is very important. So far, we have only seen three examples of fields: $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. It turns out there are many others, such as $\mathbb{Z}/5\mathbb{Z}$. So the theorem above applies for many choices of R.

Remark 12.2.5. However, you have seen that $R[x]$ is never a field (Exercise 7.5.6). In particular, the theorem does not guarantee an analogous division algorithm in $R[x][y] = R[x, y]$ with as nice a notion of remainder.

12.2.1 Division in fields

Recall that a field F is a commutative ring in which any non-zero element has a multiplicative inverse. That is, for every $x \in F$, there is some y so that $xy = yx = 1$.

It will not betray your intuition to write y as x^{-1}, or as $\frac{1}{x}$. Here are some examples justifying this:

Example 12.2.6. If $F = \mathbb{Q}$, then the multiplicative inverse of 5 is the rational number $\frac{1}{5}$.

Likewise, if $F = \mathbb{R}$, then the multiplicative inverse of π is the real number $\frac{1}{\pi}$.

Notation 12.2.7. Let F be a field, and let b be a non-zero element of F. Then we write

$$\frac{a}{b}$$

to mean the element obtained by multiplying a with the multiplicative inverse of b.

We will also write

$$b^{-1} \qquad \text{and} \qquad \frac{1}{b}$$

to denote the multiplicative inverse to b.

Example 12.2.8. This is consistent with the usual notation for rational numbers:

$$\frac{3}{5} = 3 \times \frac{1}{5}.$$

Remark 12.2.9. The intuition I want you to build is the following: *a field is a ring in which you can divide* (by non-zero elements, and always without "remainders").

Example 12.2.10. Let F be a field, let $a, b \in F$ with $b \neq 0$, and let c be the multiplicative inverse to b. Then

$$\frac{a}{b} \times b = (a \times c) \times b = a \times (c \times b) = a \times 1 = a.$$

In other words, $\frac{a}{b} \times b = a$, as you would expect from fraction notation.

12.2.2 Long division for polynomials

The proof of Theorem 12.2.3 will pass through an algorithm for dividing polynomials, which we'll call long division in analogy with usual division of numbers.

Let's first understand by example. We'll carry out the division

$$(9x^4 - 3x^3 + x^2 - 10x + 4) \div (2x^2 + 3).$$

As usual, let's start writing the usual division set-up:

$$2x^2 + 3\overline{\big)\,9x^4 - 3x^3 + x^2 - 10x + 4}$$

Division step. we focus only on the *highest order* terms of both polynomials involved: $2x^2$ and $9x^4$, in our case. And we ask, can we divide $9x^4$ by $2x^2$? The answer is yes: $\frac{9}{2}x^2$ is the quotient. You can check

$$\frac{9}{2}x^2 \cdot 2x^2 = 9x^4.$$

So we record this quotient right above the highest-order term of the dividend:

$$\begin{array}{l} \qquad\quad\;\; \tfrac{9}{2}x^2 \\ x^2 + 3\overline{\big)\,9x^4 - 3x^3 + x^2 - 10x + 4} \end{array}$$

Remark 12.2.11. Notice that at this stage, it was important that we could *divide* the coefficient 9 by the coefficient 2. In other words, we are using the fact that our coefficients take values in a field. See Remark 12.2.9.

In fact, this division step (and its repetitions later on) is the only place where we use that the base ring is a field.

Multiplication step. Now we multiply this term, $\frac{9}{2}x^2$, with the divisor, and write the result below the dividend in preparation for subtraction:

$$\begin{array}{rl} & \frac{9}{2}x^2 \\ \cline{2-2} x^2+3\big) & 9x^4 - 3x^3 + \quad x^2 - 10x + 4 \\ & 9x^4 + \quad 0 + \frac{27}{2}x^2 \end{array}$$

Note that as we write, we are lining up terms by degree.

Subtraction step. Just as with usual division of numbers, we now subtract:

$$\begin{array}{rl} & \frac{9}{2}x^2 \\ \cline{2-2} x^2+3\big) & 9x^4 - 3x^3 + \qquad x^2 - 10x + 4 \\ & 9x^4 + \quad 0 + \quad \frac{27}{2}x^2 \\ \cline{2-2} & \qquad - 3x^3 + (\frac{-25}{2})x^2 \end{array}$$

Now we repeat the process.

Division again. Again, focusing only the highest-degree term $-3x^3$ of the new polynomial and the highest-degree term x^2 of the divisor, we see that $-3x$ is the quotient:

$$(-3x) \cdot x^2 = -3x^3.$$

And we place $-3x$ atop the long division bar:

$$\begin{array}{rl} & \frac{9}{2}x^2 - \ 3x \\ \cline{2-2} x^2+3\big) & 9x^4 - 3x^3 + \qquad x^2 - 10x + 4 \\ & 9x^4 + \quad 0 + \quad \frac{27}{2}x^2 \\ \cline{2-2} & \qquad - 3x^3 + (\frac{-25}{2})x^2 \end{array}$$

Multiplication again. Now we multiply $-3x$ by the divisor, and place the result in a position ready for subtraction:

$$\begin{array}{rl} & \frac{9}{2}x^2 - \ 3x \\ \cline{2-2} x^2+3\big) & 9x^4 - 3x^3 + \qquad x^2 - 10x + 4 \\ & 9x^4 + \quad 0 + \quad \frac{27}{2}x^2 \\ \cline{2-2} & \qquad - 3x^3 + (\frac{-25}{2})x^2 \\ & \qquad - 3x^3 + \qquad 0 - \ 9x \end{array}$$

Substraction again. We subtract:

$$
\begin{array}{rlllll}
 & \frac{9}{2}x^2 - & 3x & & & \\
\cline{2-6}
x^2+3\big) & 9x^4 - & 3x^3 + & x^2 - & 10x + & 4 \\
 & 9x^4 + & 0 + & \frac{27}{2}x^2 & & \\
\cline{2-4}
 & & -3x^3 + & (\frac{-25}{2})x^2 & & \\
 & & -3x^3 + & 0 - & 9x & \\
\cline{3-5}
 & & & (\frac{-25}{2})x^2 - & x &
\end{array}
$$

Remark 12.2.12. In fact, during the subtraction step, some people like to have brought down the relevant lowest-degree term, too, so people would have written the previous step as follows (the difference is in blue):

$$
\begin{array}{rlllll}
 & \frac{9}{2}x^2 - & 3x & & & \\
\cline{2-6}
x^2+3\big) & 9x^4 - & 3x^3 + & x^2 - & 10x + & 4 \\
 & 9x^4 + & 0 + & \frac{27}{2}x^2 & & \\
\cline{2-4}
 & & -3x^3 + & (\frac{-25}{2})x^2 & -10x & \\
 & & -3x^3 + & 0 - & 9x & \\
\cline{3-5}
 & & & (\frac{-25}{2})x^2 - & x & +4
\end{array}
$$

We keep repeating, resulting in work as follows:

Division again again:

$$
\begin{array}{rlllll}
 & \frac{9}{2}x^2 - & 3x - & \frac{25}{2} & & \\
\cline{2-6}
x^2+3\big) & 9x^4 - & 3x^3 + & x^2 - & 10x + & 4 \\
 & 9x^4 + & 0 + & \frac{27}{2}x^2 & & \\
\cline{2-4}
 & & -3x^3 + & (\frac{-25}{2})x^2 & -10x & \\
 & & -3x^3 + & 0 - & 9x & \\
\cline{3-5}
 & & & (\frac{-25}{2})x^2 - & x & +4
\end{array}
$$

Multiplication again again:

$$
\begin{array}{rlllll}
 & \frac{9}{2}x^2 - & 3x - & \frac{25}{2} & & \\ \cline{2-6}
x^2+3\big) & 9x^4 - & 3x^3 + & x^2 - & 10x + & 4 \\
 & 9x^4 + & 0 + & \frac{27}{2}x^2 & & \\ \cline{2-4}
 & & -3x^3 + & (\frac{-25}{2})x^2 - & 10x & \\
 & & -3x^3 + & 0 - & 9x & \\ \cline{3-5}
 & & & (\frac{-25}{2})x^2 - & x + & 4 \\
 & & & (\frac{-25}{2})x^2 + & \frac{-75}{2}x &
\end{array}
$$

Subtraction again again:

$$
\begin{array}{rlllll}
 & \frac{9}{2}x^2 - & 3x - & \frac{25}{2} & & \\ \cline{2-6}
x^2+3\big) & 9x^4 - & 3x^3 + & x^2 - & 10x + & 4 \\
 & 9x^4 + & 0 + & \frac{27}{2}x^2 & & \\ \cline{2-4}
 & & -3x^3 + & (\frac{-25}{2})x^2 - & 10x & \\
 & & -3x^3 + & 0 - & 9x & \\ \cline{3-5}
 & & & (\frac{-25}{2})x^2 - & x + & 4 \\
 & & & (\frac{-25}{2})x^2 + & \frac{-75}{2}x & \\ \cline{4-6}
 & & & & \frac{73}{2}x + & 4
\end{array}
$$

And we are finally finished when, at the bottom, we end up with a polynomial whose degree is less than the degree of the divisor. In this case, $\frac{73}{2}x - 4$ has degree less than $x^2 + 3$. What we conclude is

$$9x^4 - 3x^3 + x^2 - 10x + 4 = (\frac{9}{2}x^2 - 3x - \frac{25}{2})(x^2 + 3) + (\frac{73}{2}x + 4).$$

So the remainder r is the polynomial

$$\frac{73}{2}x + 4.$$

In the notation of the theorem, q is the polynomial

$$\frac{9}{2}x^2 - 3x - \frac{25}{2}.$$

12.3 Proof of Theorem 12.2.3

First, let us note that the division algorithm always terminates (i.e., it does not go on forever). The reason is as follows.

Noting that the division algorithm repeats the divide-multiply-subtract cycle over and over, we observe that the ith cycle begins by trying to divide some polynomial p_i by the divisor. (In the worked-out example above, in the 1st cycle, we were dividing $p_1 = 9x^4 - 3x^3 + x^2 - 10x + 4$. In the 2nd cycle, we were dividing $p_2 = -3x^3 + (\frac{-25}{2})x^2 - 10x$, and in the third cycle, we were dividing $p_3 = (\frac{-25}{2})x^2 - x - 4$; all by $x^2 + 3$.)

Then p_i always has smaller degree than p_{i-1}. This is because—by the design of the multiplication and subtraction step—p_i is obtained from p_{i-1} by subtracting off a polynomial whose top degree term agrees with the top degree term of p_{i-1}.

So, if the original dividend $a = p_1$ has degree n, and if the divisor b has degree m, then after at most $i = n - m + 1$ cycles, we see that p_i has degree strictly less than m, at which point the division algorithm stops because a degree m polynomial b cannot factor into a polynomial p_i of lesser degree. (After all, degrees *add* when we multiply polynomials—see Proposition 7.3.25.)

We have finished our proof that the division algorithm terminates. It is a tedious exercise in the distributive property to verify that the algorithm indeed produces polynomials q (the quotient) and r (the remainder) for which

$$a = qb + r.$$

We leave this tedious verification to our dear reader.

Now let us prove uniqueness. Suppose q' and r' are two other polynomials, with $\deg(r') < \deg(b)$, satisfying $a = q'b + r'$. Then we have that

$$(q - q')b = r - r'.$$

Now, the righthand side is a polynomial of degree strictly less than $\deg b$. On the other hand, the lefthand side is a polynomial of degree at least b *unless* $q - q' = 0$. Thus, we conclude $q - q' = 0$, meaning $q = q'$. It follows that r must equal r', completing the proof.

12.4 Using a zero of a polynomial to factor

That we can divide polynomials with remainders (Theorem 12.2.3) is incredibly powerful. Here we record some useful corollaries.

Remark 12.4.1. In fact, the corollaries below are true even if R is just an integral domain, and not a field. The reason is that in all the polynomial divisions we perform in proving the corollaries, the divisor is always a polynomial whose highest-degree coefficient is 1; and we can always divide by 1, field or not.

Corollary 12.4.2. Let R be a field and fix a polynomial $a \in R[x]$. Suppose that for some value $x_0 \in R$, we know that $a(x_0) = 0$. Then there exists some polynomial $q(x)$ for which

$$a(x) = q(x)(x - x_0).$$

Proof. Setting $b = x - x_0$, we may use Theorem 12.2.3 to conclude there must exist q and r so that

$$a(x) = q(x)(x - x_0) + r(x). \tag{12.4.0.1}$$

Moreover, since[1] $\deg(b) = \deg(x - x_0) = 1$, we know that $r(x)$ must have degree 0 (or $-\infty$, if $r = 0$). In particular, $r(x)$ is a constant polynomial, and we may write $r(x) = C$ for some constant C. We are finished if we can prove $C = 0$.

Well, let us plug in the value $x = x_0$. Then (12.4.0.1) becomes

$$a(x_0) = q(x_0)(x_0 - x_0) + C.$$

Note that the hypothesis of the corollary tells us that $a(x_0) = 0$. On the other hand, $x_0 - x_0 = 0$. So we have

$$0 = 0 + C.$$

This shows $C = 0$. □

Corollary 12.4.3. Let R be a field and fix a degree n polynomial a. Suppose that there are n distinct elements $x_1, \ldots, x_n \in R$ for which $a(x_i) = 0$. Then

$$a(x) = C(x - x_1)(x - x_2) \ldots (x - x_n)$$

for some constant $C \in R$.

[1] Note that x_0 is a constant (i.e., an element of the base ring R) while x is a variable.

Proof. We proceed by induction on the degree of a, with base case $\deg a = 1$.

If $\deg a = 1$, Corollary 12.4.2 gives us the result we seek (by noting that $\deg q$ must be 0.)

For the inductive step, let us assume we have proven the result for all degree $n - 1$ polynomials. Given a degree n polynomial a with zeroes as stated in the hypothesis, we use Corollary 12.4.2 to conclude

$$a(x) = q(x)(x - x_n)$$

where q has degree $n - 1$. But because R is a field (and in particular, an integral domain) the fact that $a(x_i) = 0$ but $(x_i - x_n) \neq 0$ means $q(x_i)$ must equal zero. So the $x_1, \ldots, x_{n-1}$ are zeroes of q, and the inductive hypothesis tells us

$$q(x) = C(x - x_1) \ldots (x - x_{n-1}).$$

Combining the above two centered equations, we are finished. □

12.5 Exercises

Exercise 12.5.1. (a) Write out the addition and multiplication tables for $\mathbb{Z}/7\mathbb{Z}$.

(b) Which elements of $\mathbb{Z}/7\mathbb{Z}$ have multiplicative inverses?

(c) Which elements of $\mathbb{Z}/7\mathbb{Z}$ have square roots?

(d) Is $\mathbb{Z}/7\mathbb{Z}$ an integral domain?

(e) Is $\mathbb{Z}/7\mathbb{Z}$ a field?

Exercise 12.5.2. (a) Write out the addition and multiplication tables for $\mathbb{Z}/8\mathbb{Z}$.

(b) Which elements of $\mathbb{Z}/8\mathbb{Z}$ have multiplicative inverses?

(c) Which elements of $\mathbb{Z}/8\mathbb{Z}$ have square roots?

(d) Is $\mathbb{Z}/8\mathbb{Z}$ an integral domain?

(e) Is $\mathbb{Z}/8\mathbb{Z}$ a field?

Exercise 12.5.3. Let n be an integer with $n \geq 3$.

(a) Show that there is at least one element $a \in n$ for which the equation $x^2 - a = 0$ has no solution in $\mathbb{Z}/n\mathbb{Z}$. (In other words, prove that there is at least one element of $\mathbb{Z}/n\mathbb{Z}$ that is not a square; i.e., that has no square root in $\mathbb{Z}/n\mathbb{Z}$.)

(b) In fact, show that at most $(n+1)/2$ elements of $\mathbb{Z}/n\mathbb{Z}$ are squares.

Exercise 12.5.4. Let $a(x) = 3+4x-7x^5$, and let $b(x) = 3x^3-2x+1$. Note that you can consider these as polynomials with coefficients in $\mathbb{Z}/n\mathbb{Z}$ for any n, by simply thinking of a coefficient as the equivalence class represented by the coefficient. (So for example, think of -7 as $[-7]$.)

Using the division algorithm for polynomials, for each of the following values of n, compute the polynomials $q(x), r(x) \in \mathbb{Z}/n\mathbb{Z}$ for which $a(x) = q(x)b(x) + r(x)$ and $\deg r < \deg b$.

(a) $n = 2$

(b) $n = 3$

(c) $n = 5$

(d) $n = 7$.

(You may need to think about what the multiplicative inverse to some numbers are in each of the rings $\mathbb{Z}/n\mathbb{Z}$ above.)

Exercise 12.5.5. Let $R = \mathbb{Z}/5\mathbb{Z}$. Note that 2 is not a square in R (for example, by looking at the multiplication table of $\mathbb{Z}/5\mathbb{Z}$). So the polynomial $x^2 - 2$ has no solution in R.

Consider the quotient ring $S = (\mathbb{Z}/5\mathbb{Z})[x]/(x^2-2)$. (That is, one considers polynomials with coefficients in $\mathbb{Z}/5\mathbb{Z}$, then quotients this polynomial ring by the principal ideal generated by $x^2 - 2$.)

(a) How many elements does S contain? (Hint: Use the division algorithm to see that every equivalence class has exactly one representative of degree ≤ 1.)

(b) In the ring S, is there some element that squares to 2?

(c) Prove or disprove: S is a field.

12.6 Extra Credit

(a) Prove that if p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field. (If you prove this, you will have shown that for any prime number p, there exists a field with p elements.) Hint: This will require the Euclidean algorithm, see Exercise 9.9.2.

(b) Let p be any prime number. By combining Exercise 12.5.3 with ideas from Exercise 12.5.5, show that there exists a field with exactly p^2 elements.

Note: It turns out that (i) For every $k \geq 1$, there is a field with p^k elements, and (ii) If F is a finite field, then F has p^k elements for some prime p and some integer $k \geq 1$. We don't quite have the machinery to prove these claims yet.

12.7 Idea map assignment

We have now completed the portion of our course that focuses on rings.

For this assignment, I want you to make a graphical representation of the ideas we've learned so far.

Below are fewer than 40 key ideas and terms we've talked about.

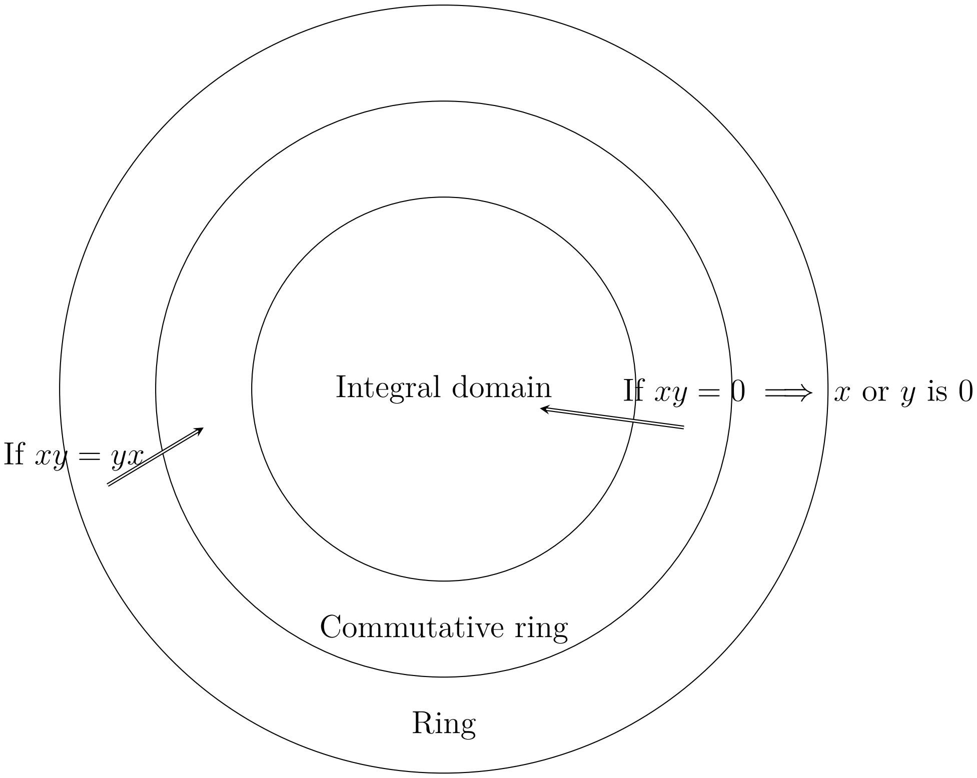
Prompt. I want you to make an "idea map" either by hand or digitally. An idea map is a visual representation expressing the relationships between various ideas. I'd like you, on this idea map, to include at least 20 of the ideas/terms below, and indicate how[2] they are connected to each other.

Example 12.7.1. For example, your representation may just look like a graph with lines between them, with lines indicating some "connection." But in drawing this connection, you must indicate what the connection actually is. For example:

$$\text{Ring} \xrightarrow{\text{If } xy = yx} \text{Commutative ring} \xrightarrow{\text{If } xy = 0 \implies x \text{ or } y \text{ is } 0} \text{Integral domain}$$

[2] This means just drawing arrows/bridges/lines is not enough—you must verbally or otherwise communicate what substantiates those arrows, or what the connections are.

The same connections might be drawn as follows:



Be creative, and feel free to run wild. At the same time, do not plan for anything too grandiose. It is more important to get the connections laid out than to make things look nice.

The terms/ideas, grouped by some arbitrary associations:

(A) (a) Ring
  (b) Commutative Ring
  (c) Integral domain
  (d) Field

(B) (a) Multiplicative identity
  (b) Additive identity
  (c) Additive inverse

(C) (a) Commutativity of addition

- (b) Associativity of addition
- (c) Associativity of Multiplication
- (d) Distributivity of multiplication over addition

(D)
- (a) $R[x]$
- (b) $R[x_1, \ldots, x_n]$
- (c) $M_2(\mathbb{R})$
- (d) $\mathbb{C}$
- (e) $\mathbb{Z}$
- (f) $\mathbb{Q}$
- (g) $\mathbb{R}$
- (h) $\mathbb{Z}/n\mathbb{Z}$
- (i) $\mathbb{Z}/p\mathbb{Z}$

(E)
- (a) Prime ideal

(F)
- (a) Algebraic set
- (b) Algebraic function
- (c) Ideal

(G)
- (a) Equivalence relation
- (b) Equivalence class
- (c) Quotient map
- (d) Ideal
- (e) Quotient ring

(H)
- (a) Universal property of quotient rings

(I)
- (a) Ring homomorphism
- (b) Ring isomorphism

(J)
- (a) Action of $\mathbb{C}$ on $\mathbb{R}^2$
- (b) Action of $M_2(\mathbb{R})$ on $\mathbb{R}^2$