Maximal ideals

Acknowledgements

Veronica mentioned this proof would be helpful to motivate. Then, Tim and Veronica wrote up some motivations for it. And Fredy pointed out that this problem is an example of learning from failure.

The problem

Consider a commutative ring R. (Remember, in rings, addition is always commutative. So here, we're saying multiplication is also).

Prove that R/I is a field $\iff$ I is a maximal ideal (that is, an ideal containing I and any other element would be the whole ring) .

An example

Consider the ring of integers: $\mathbb{Z}$.

The maximal ideals are the prime number ideals (e.g. $2\mathbb{Z}$, $3\mathbb{Z}$, $5\mathbb{Z}$). And indeed, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/5\mathbb{Z}$ are fields.

(The $\implies$ direction) R/I is a field $\implies$ I is a maximal ideal

Our problem start state is:

$$R : \textit{commutative ring}$$

$$I : \textit{ideal of } R$$

$$R/I : \textit{field}$$

$$=========$$

$$I : \textit{maximal ideal of } R$$

We can rewrite the conclusion: So we want to show that if we consider an ideal J that contains I and one more element x that's not in I, then 1 will be in J, so we get the whole ring.

So now we have:

$$R : \textit{commutative ring}$$

$$I : \textit{ideal of } R$$

$$x \in R, x \notin I$$

$$J : \textit{ideal of } R$$

$$J \supseteq I \cup \{x\}$$

$$R/I : field$$

$$=========$$

$$1 \in J$$

We can rewrite the hypothesis, too: Since R/I is a field, we know for any element in R/I, there is a multiplicative inverse. So, for the coset of any element (call it a), there exists a coset of an element b that gives the identity.

So now we have:

$$R : \textit{commutative ring}$$

$$I : \textit{ideal of } R$$

$$x \in R, x \notin I$$

$$J : \textit{ideal of } R$$

$$J \supseteq I \cup \{x\}$$

$$\forall (a + I) \in R/I, \exists (b + I) \in R/I, (a + I)(b + I) = (1 + I)$$

$$=========$$

$$1 \in J$$

We are tempted to find the multiplicative inverse of the coset of our previously chosen x…

$$R : \textit{commutative ring}$$

$$I : \textit{ideal of } R$$

$$x \in R, x \notin I$$

$$J : ideal\ of\ R$$

$$J \supseteq I \cup \{x\}$$

$$\exists (y + I) \in R/I, (x + I)(y + I) = (1 + I)$$

=========

$$1 \in J$$

But it's not entirely straightforward how to make progress from here.

A failing conjecture

Note that the *cosets* of x and y being multiplicative inverses in R/I does not mean the *elements* x and y are multiplicative inverses in the ring R. For example, when we consider $\mathbb{Z}/7\mathbb{Z}$, the coset $(2 + 7\mathbb{Z})$ has a multiplicative inverse $(4 + 7\mathbb{Z})$, but 2 and 4 are not multiplicative inverses in the full ring $\mathbb{Z}$.

What we do have, though, is there's an element in the coset of 2 and an element in the coset of 4 that multiplies to an element in the coset of 1. (2 times 4 equals 8, which is in the coset of 1).

Takeaway from the failure

And so in general, for our problem, we have that there exists some $a \in (x + I) \subseteq J$ (that is, some element "a" that is a "multiple" of x…which will be in J since all multiples of x will be in J), and some $b \in (y + I) \subseteq R$ (that is, some element "b" that is a "multiple" of y) and $i \in I$ such that $ab = 1 + i$.

That is $\exists a \in J, b \in R, i \in I$ such that:

$$ab - i = 1$$

And since $a \in J$ and $b \in R$, then $ab \in J$. And $i \in J$.

So $ab - i = 1 \in J$.

So, J must be the whole ring. □

(The $\Longleftarrow$ direction) I is a maximal ideal $\Longrightarrow$ R/I is a field

Here, it's helpful to take the contrapositive.

We assume that R/I is not a field, and want to prove I is not maximal.

We can motivate taking the contrapositive since it turns a "for all statement" (every non-zero element in R/I has a multiplicative inverse) to an "existence" statement (there is one non-zero element in R/I that has no multiplicative inverse).

So, consider the non-zero element $(x + I)$ in R/I with no multiplicative inverse. Formally:

$$\exists (x + I) \neq 0 \in R/I, \forall (y + I) \in R/I, (x + I)(y + I) \neq (1 + I)$$

Here, it helps to look at a particular example. Is anything special happening among the elements with no multiplicative inverse?

The non-invertible elements of the quotient ring are 2,4, and 6. Indeed, if we add any of those elements to the ideal, we get the ideal $2\mathbb{Z}$ or $4\mathbb{Z}$, which are ideals which strictly contain $8\mathbb{Z}$ but are strictly contained in the full ring of integers.

So:

- Call $(x + I)$ any non-invertible element of the quotient ring (and non-field) R/I.
- Let x be any element of that coset $(x + I)$.
- Now we can conjecture. If we consider the smallest ideal (call it J) containing I and that non-invertible x…

  $$J := \textit{ideal generated by } I \textit{ and } \{x\}$$

  …then

  $$I \subsetneq J \subsetneq R$$

  and therefore I is not maximal.

Let's prove it.

- *J is a proper superset of I.*
    - We know (x+I) is a non-zero element in R/I. It's non-zero by assumption — we chose it to be the non-zero element in R/I with no multiplicative inverse.

- All of the elements in I get sent to one coset — the zero coset.
- But (x+I) is not in that coset. So, x is not in I.

- *J is a proper subset of R.*
  - Suppose J did contain 1 (the multiplicative identity of R, and therefore was all of R).
  - I initially started to write J as all elements of the form polynomials of x (e.g. any element in J takes the form $a + bx + cx^2 + ...$). But I couldn't get any contradiction by setting one of these elements equal to 1.
  - But the big hint here is realizing that J can be written much more simply, as:

    $$J := \{rx + i : r \in R, i \in I\}$$

    You can prove this by noticing that:

    - J is an ideal (since if $r_0 \in R$, then $r_0(rx + i) = r_0rx + r_0i$ which is still in J).
    - J contains I and x.
    - (You can also prove that J is the *smallest* ideal containing $I$and x, but you might realize later on you don't even have to, because whether this construction of J is minimal or not, it satisfies $I \subsetneq J \subsetneq R$.)
  - With that hint, you can recognize that if 1 was in J, then that means there exists some r and i such that $rx + i = 1$, which means $(rx + I) = (1 + I)$, which means $(r + I)(x + I) = (1 + I)$, which means $(x + I)$ is invertible. That's a contradiction, and so J must be a proper subset of R. $\square$