Let $\phi : D \to F, a \mapsto [(a, 1)]$ is a ring homomorphism. Clearly,

$$\phi(a + b) = [(a + b), 1] = [(a1 + 1b, 1)] = [(a, 1)] + [(b, 1)] = \phi(a) + \phi(b)$$

and

$$\phi(a \times b) = [(ab, 1)] = [(a, 1)] \times [(b, 1)] = \phi(a)\phi(b).$$

To show injectivity, let's look at $\ker \phi$:

$$\ker \phi = \{a \in D : \phi(a) = 0\} = \{a \in D : [(a, 1)] = [(0, 1)]\}.$$

iff $a = 0$. So $\ker \phi = \{e\}$.

Theorem

If F is the field of fraction of D, and K is some other field containing D, then K has a subfield isomorphic to F.

Intuition. If $\iota : D \to K$ is an injective map.

$$\iota\left(\frac{a}{b}\right) \to \frac{\iota(a)}{\iota(b)} = \iota(a)(\iota(b))^{-1}.$$

How do we check that F is the field of fractions of D?

We need to check

1) F is a field.
2) "F is not too small".
3) "F is not too big". $\mathbb{R}$ isn't the field of fractions of $\mathbb{Z}$ because $\pi \in \mathbb{R}$ but $\pi \neq \frac{a}{b}$ for $a, b \in \mathbb{Z}, b \neq 0$.

Example (21.1)**.** $D = \{n + m1, : n, m \in \mathbb{Z}\}$ Gaussian integers.

Why is this a ring? Prove it's a subring of $\mathbb{C}$: closed under $+, -, \times$ and nonempty.

Why is this a domain? D is commutative inherited from complex numbers. D has identity $(1 + 0i)$. And D has no zero divisors because $\mathbb{C}$ is a field and doesn't.

The field of fraction of D must be a subring of $\mathbb{C}$. We guess that

$$F = \{p + qi : p, q \in \mathbb{Q}\}$$

is the field of fractions.

F is a field (done in previous homeowkr). F is a subring. It is commutative and has identity. Every element has inverse.

F needs to contain D. Clearly $D \subseteq F$ because $\mathbb{Z} \subseteq \mathbb{Q}$.

F is not too big: Every element of F is of form $\frac{a}{b}, a, b \in D, b \neq 0$. Given $p + qi \in F$, express this as $\frac{a+bi}{c+di}$ where $a, b, c, d \in \mathbb{Z}$. If $p + qi = \frac{r}{s} + \frac{t}{u}i$ with $r, s, t, u \in \mathbb{Z}$ and $s, u \neq 0$.

$$\frac{r}{s} + \frac{t}{u}i = \frac{ru + sti}{su + 0i}.$$

Example. What is the field of fraction of $\mathbb{Q}$? It is $\mathbb{Q}$ itself.

22: Polynomial Rings

Start with a ring R (probability commutative with identity). Invent a new ring $R[x]$ (polynomials with coefficients in R in the indeterminate x).

Warning: x is NOT a variable. It is not waiting for you to plug in a value. "Plugging in values" is only allowed in the context of evaluate homomorphisms. x is just x.

A typical element of $R[x]$ looks like

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n.$$

where $n \in \mathbb{N}, a_i \in R$. We don't allow infinite terms because we don't want infinitely many coefficients.

Note

$$a_0 + \ldots + a_nx^n = b_0 + \ldots + b_nx^n \Leftrightarrow a_i = b_i \ \forall \ i.$$

In fact, $1 - x^2 = 1 + 0x - x^2 + 0x^3$.

These polynomials are not functions! Consider $\mathbb{Z}_3[x]$. $x^3 - x + 1, 1 \in \mathbb{Z}_3[x]$. If we illegally plug in values 0,1,2, then the outputs equal but they aren't functions. This is happening because every element of $\mathbb{Z}_3$ is a root of $x^3 - x$. This cannot happen in infinite fields like $\mathbb{Z}$. We need to check coefficients instead and they clearly aren't the same.

Addition:

$$\sum_{i=0}^{n} a_ix^i + \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{n} (a_i + b_i)x^i.$$