Math 3032   Jan 31, 2023

No office hours this week except by appt.

Next week: in person in LSC C202.

Last time we studied the ring

$$\mathbb{Z}[\sqrt{-7}] \text{ subring where } a,b \text{ both } \in \mathbb{Z}$$

$$R = \{ a + b\sqrt{-7} \text{ s.t. } a,b \text{ both } \in \mathbb{Z} \text{ or } a,b \text{ both } \in \mathbb{Z}+\tfrac{1}{2} \}.$$

$$R \subseteq \mathbb{C}$$

$$R = \mathbb{Z}\left[\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-7}\right]$$

If $a + b\sqrt{-7} \in R$,

try to solve

$$a + b\sqrt{-7} = a' + b'\left(\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-7}\right) \text{ for } a', b'.$$

answer: $b' = 2 \cdot b$. $a' = a - b$.] ← both in $\mathbb{Z}$!

What do ideals in R look like?

(1)

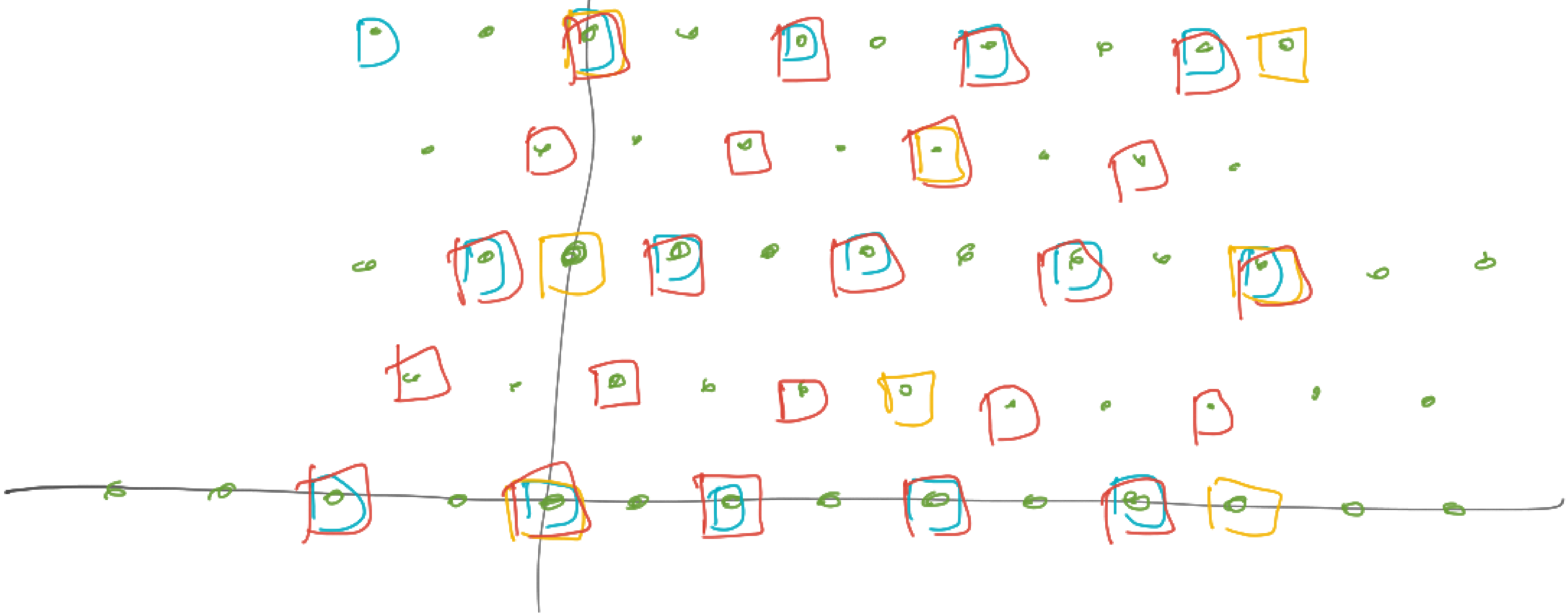
(2)

$(\sqrt{-7})$

$(\frac{1}{2}+\frac{\sqrt{-7}}{2}) \supseteq (2)$

$$\left(\frac{1}{2}+\frac{\sqrt{-7}}{2}\right)\left(\frac{1}{2}-\frac{\sqrt{-7}}{2}\right)$$

$$= \frac{1}{4}+\frac{7}{4}+\cancel{\frac{\sqrt{-7}}{4}}-\cancel{\frac{\sqrt{-7}}{4}} = 2$$



Principal ideals: rescaled + rotated copies of R.

What does "$\mathbb{Z}[\sqrt[3]{4}]$" mean?

Idea: all "numbers" that can be built by $\mathbb{Z}$, $\sqrt[3]{4}$ from $\times, +, -$. (no division).

$$\underset{+4a}{a} + b\sqrt[3]{4} + c\underbrace{(\sqrt[3]{4})^2}_{=\,2\sqrt[3]{2}} + \cancel{d\underbrace{(\sqrt[3]{4})^3}_{=\,4}}$$

$$(a + b\sqrt[3]{4} + 2c\sqrt[3]{2})(a' + b'\sqrt[3]{4} + 2c'\sqrt[3]{2})$$

$$= (aa' + 4bc' + 4b'c) + (ab' + ba' + 4cc')\sqrt[3]{4} + 2(ac' + bb' + ca')\sqrt[3]{2}$$

$\mathbb{Z}[\sqrt[3]{4}] = \{a + b\sqrt[3]{4} + 2c\sqrt[3]{2}$ s.t. $a, b, c \in \mathbb{Z}\} \subseteq \mathbb{R}$.

What are polynomials?

Let R be a ring.

Then

$$R[x] = \left\{ \begin{array}{l} \text{(infinite) sequences } (a_0, a_1, a_2, \dots) \\ \quad \text{all } a_i \in R \\ \text{s.t. } \exists N \text{ s.t. } a_i = 0 \ \forall i > N. \end{array} \right\}$$

"finite length sequences".

Notation:

$$(a_0, a_1, a_2, \dots) \rightsquigarrow a_0 + a_1 x + a_2 x^2 + \dots$$

So far, "x" is just notational bookkeeping.

We'll assign $+, \times$. That will give meaning to the syntax.

<u>$+$:</u> sum term by term.

$$\begin{array}{r} (a_0, a_1, a_2, \dots) \\ + \ (b_0, b_1, b_2, \dots) \\ \hline (a_0+b_0, a_1+b_1, a_2+b_2, \dots) \end{array}$$

For this to be valid: have to convince that if $a_i = 0$ after some cut off and $b_i = 0$ after some possibly dif. cut-off, then $a_i + b_i$ is eventually zero.

i.e.

$$\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) = \sum_i (a_i + b_i) x^i.$$

<u>Pf:</u> use larger of the two cutoffs.

$\underline{X:}$ want: $x^m \cdot x^n = x^{m+n}$.

The rule is: the k-th entry of
$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots)$

is

$$\sum_{\substack{i,j \in \mathbb{N} \\ \text{s.t.} \\ i+j=k}} a_i \cdot b_j.$$

For this to be valid:

* $\sum_{\substack{i,j \in \mathbb{N} \\ i+j=k}} a_i \cdot b_j \in R$?

Yes: this is a sum of $k+1 < \infty$.

* product sequence is eventually zero.

$\mathbb{N} = \{0, 1, 2, \dots\} \subseteq \mathbb{Z}$

Defn: Suppose $p(x) \in R[x]$.

Does not mean a function!

"$p(x)$" is a formal expression of shape $a_0 + a_1 x + \dots + a_n x^n + \dots$ eventually zeros.

Say $p(x)$ has degree $\leq N$ if ith coef $a_i = 0$ $\forall i > N$.

$deg(p) = N$ if $deg(p) \leq N$ and $deg(p) \nleq N_{-1}$.

E.g. $1 + x +$ rest zeros. has degree ≤ 5.

Lemma: If $deg(p) \leq N$ and $deg(q) \leq M$, then $deg(p+q) \leq max(N, M)$, $deg(p \cdot q) \leq N + M$.

$\{$polys of deg $\leq N\}$ is an additive subgp of $R[x]$

$\{$polys of deg $= N\}$ is not closed under $+$.

$$\underset{\deg = n}{x^n} + \underset{\deg = n}{(-x^n)} = \underset{\deg = ?}{0}$$

Convention: $\deg(0) = -\infty$.

Defined $R[x]$: I gave $+, \times$.

Is it a ring? Yes. gp under $+$? yes, e.g. $-(a_0, a_1, \ldots) = (-a_0, -a_1, \ldots)$

e.g. assoc?

$$\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right)\left(\sum_k c_k x^k\right)$$

claim: w/ either parenthesizing $\underbrace{(\cdot\,\cdot)\cdot}$ $-$ $\underbrace{\cdot(\cdot\,\cdot)}$

answer is: ℓ^{th} coeff

$$\sum_\ell \Big(\qquad\qquad \Big) x^\ell$$

$$\| $$

$$\sum_{\substack{i,j,k \\ \text{s.t.} \\ i+j+k=\ell}} (a_i b_j) c_k .$$

use R itself is assoc.

also use: R is distributive.

Lemma:

Iff R is

- unital
- com.
- integral domain

then so is $R[x]$.

these are poly's of deg ≤ 0.

$1 = 1 + 0x + 0x^2 + \dots$ is unit for $R[x]$.

if $a, b \neq 0$, then $ab \neq 0$.

$R \subseteq R[x]$ is a subring,

$r \mapsto r + 0x + 0x^2 + \dots$

pf: Suppose $\sum a_i x^i$, $\sum b_j x^j$ both not zero.

Let $n = \deg(\sum a_i x^i)$, $m = \deg(\sum b_j x^j)$.

then $(m+n)$th coef in $(\sum a_i x^i)(\sum b_j x^j) = a_n \cdot b_m$.

by defn of deg, a_n, b_m both not zero, so $a_n b_m \neq 0$.

so $(\ )(\ ) \neq 0$.

$\lightning$ polynomials $\neq$ functions!

Let R be a ring.

Claim: $\exists$ a unique ring hom

$$R[x] \xrightarrow{\text{"ev"}} \{\text{functions } R \to R\}.$$

$\uparrow$ this is a ring!

given functions f, g,

define $f+g : r \mapsto f(r)+g(r)$

$f \cdot g : r \mapsto f(r) \cdot g(r)$.

with the properties

"x" $\longmapsto$ the function w/ formula "x"

aka the identity function.

$r + 0x + 0x^2 + \ldots \longmapsto$ constant function w/ value r. $\quad \forall r \in R$.

$R = \mathbb{Z}_p$. $\quad p$ a prime. $\left(\begin{array}{c}\text{in particular} \\ p \neq 1\end{array}\right)$

$x^p - x \longmapsto 0 \in \{\text{functions } R \to R\}$.

$\neq$
0
in $R[x]$

FLT

<u>Claim</u>: $\forall\, r \in \mathbb{Z}_p,\ r^p - r = 0$.

<u>Equiv</u>: $\forall\, r \in \mathbb{Z}_p,\ r^p = r$.

<u>Equiv</u>, $\forall\, n \in \mathbb{Z},\ n^p \equiv n \pmod p$.

<u>Pf</u>: . If $r = 0$, $0^p = 0$ ✓. Using: $\mathbb{Z}_p$ is a field!

. If $r \neq 0$, then $r \in \mathbb{Z}_p^\times$ ← abelian gp of non-zeros.

This gp has $p-1$ elts. So $r^{p-1} = 1$ in this gp. $\square$.

Remark: Same pf shows that

$$\begin{array}{ccc} x^4 - x & \longmapsto & 0 \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ \mathbb{F}_4[x] & & \text{functions } \mathbb{F}_4 \to \mathbb{F}_4 \end{array}$$

$\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ an interesting field w/ 4 elts.

OTOH: Calculus $\Rightarrow$ for $R = \mathbb{R}, \mathbb{Q}, \mathbb{C}, \ldots$

if $\underset{\in R[x]}{p(x)} \longmapsto 0$ function, then $p = 0$ poly.

Let R, S be two rings.

$$\hom(R[x], S) = ?$$

$$\begin{tikzcd}
 & \hom(R[x], S) \arrow[dl, "\substack{\varphi : R[x] \to S \\ \text{ev on } R \subseteq R[x]}"'] \arrow[dr, "\substack{\varphi \mapsto \text{ev on ``}x\text{''} \\ \varphi(x)}"] & \\
\hom(R, S) & & S
\end{tikzcd}$$

<u>Claim:</u> If S is com, then the joint map

$$\hom(R[x], S) \longrightarrow \hom(R, S) \times S$$

is a bijection.

In other words:

$\forall$ hom $R \xrightarrow{\phi} S$

and $\forall$ $s \in S$

$\exists !$ hom $R[x] \xrightarrow{\Phi} S$ s.t. $\Phi(\underset{\text{constant poly}}{r}) = \phi(r)$

and $\Phi(x) = s$.

in $R[x]$,

$x^j \cdot a_i x^i =$

$a_i x^{i+j} = a_i x^i \, x^j$

I do need s to commute w/ im(ϕ)

$\Phi(a_0 + a_1 x + a_2 x^2 + \dots) =$

$\phi(a_0) + \phi(a_1) s + \phi(a_2) s^2 + \dots$