Math 3032 Lecture 11 (25 Feb 2021)

OH next week: Tuesday 12-2.

HW 5 due today. HW 6 posted, due next week.

"$rI \subseteq I$"
Given $r \in R$
rI
$=$
$\{r \cdot a \mid a \in I\}$
$\subseteq R$

"$rI \subseteq I$" means if $a \in I$ then $ra \in I$.

equiv if R is com.

two-sided

Defn: An ideal in a ring R is an additive subgp $I \subseteq R$ s.t. $\forall r \in R$

$rI \subseteq I$ and $Ir \subseteq I$

just this condition ← "left ideal"

just this ← right ideal

two-sided $\iff$ both left and right.

E.g.: What are all ideals in $\mathbb{Z}$?

If $I \subseteq \mathbb{Z}$ ideal, then a subgp. so $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

$= (-n)\mathbb{Z}$ (because -1 is a unit).

$= (n)$

$\mathbb{Z}/(n) = \mathbb{Z}_n$.

$\mathbb{Z}/(0) = \mathbb{Z}$.

Is $n\mathbb{Z}$ an ideal? Yes: Let $r \in \mathbb{Z}$ arbitrary and $a \in n\mathbb{Z}$, i.e. $(a = n \cdot b.)$

then $ra = n \cdot rb \in n\mathbb{Z}$.

In general: if R is commutative, and choose $f \in R$.

Then (f) "principal ideal" is an ideal.

$= \{f \cdot g : g \in R\} \subseteq R$

In general: if R is commutative, and choose $f \in R$

Then (f) "principal ideal" is an ideal.

$$= \{ f \cdot g : g \in R \} \subseteq R$$

$\forall r \in R$, $r \cdot (f) \subseteq (f)$ i.e. $r f g = f \cdot rg \in (f)$.

Is it an additive gp? Yes: $f \cdot g_1 + f \cdot g_2 = f \cdot (g_1 + g_2)$.

In the case of $\mathbb{Z}$, every ideal is principal.

In most rings this is not true. (e.g. $\mathbb{Z}[x]$)

A principal ideal ring is one where every ideal is princ.

principal ideal domain is one where + no zero-divs.

E.g: What are all ideals in $\mathbb{Z} \times \mathbb{Z}$?

Say $I \subseteq \mathbb{Z} \times \mathbb{Z}$. ($I$: ideal) Pick $(x, y) \in I$ $x, y \in \mathbb{Z}$.

Take $r = (1, 0)$. $r \cdot (x, y)$ must be in I.

$\|$

$(x, 0)$. So also any multiple $(xm, 0)$

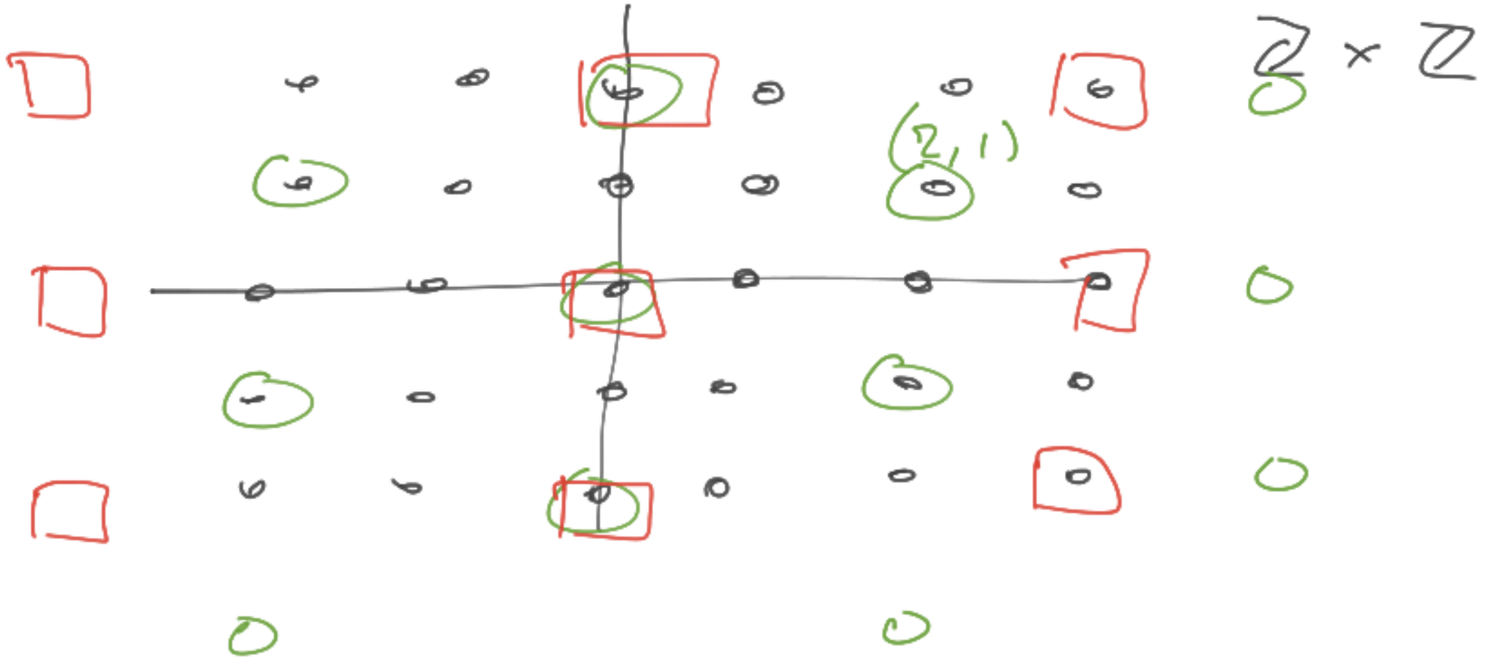
if we took $r = (0, 1)$, we'd find $(0,1) \cdot (x, y) = (0, y)$ must be in I.

There must be some $a \in \mathbb{Z}$ s.t.

$I \cap (\mathbb{Z} \times \{0\}) = \{(am, 0) : m \in \mathbb{Z}\}$

Similarly $\exists\ b \in \mathbb{Z}$ s.t. $I \cap (\{0\} \times \mathbb{Z}) = ((0, b))$

$I = (a) \times (b)$ cartesian product of ideals.



$\mathbb{Z} \times \mathbb{Z}$

● are an additive subgp.
not an ideal.

$\square = (3) \times (2)$
is an ideal.

Recall: $I \subseteq R$ ideal $\rightsquigarrow$ get quotient r.g
R/I.

$$\mathbb{Z} \times \mathbb{Z} \,/\, (a) \times (b) \cong \mathbb{Z}_a \times \mathbb{Z}_b.$$

Eg. 2:

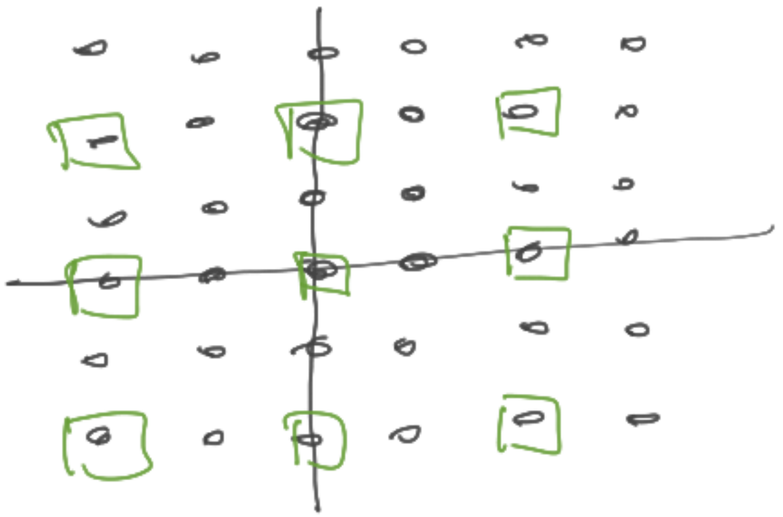
$R = \mathbb{Z}[i]$ Gaussian integers.

$= \{ a+ib : a,b \in \mathbb{Z} \} \subseteq \mathbb{C}$.

no zero-dvs.

$(a+ib)(a'+ib') = (aa' - bb') + (ab' + ba')i$.

$\mathbb{C}$



$I = (2)$ principal ideal.

$(\mathbb{Z}[i]/(2), +) \cong \mathbb{Z}_2^2$ as additive gps.

equiv classes:

$[0], [1], [i], [1+i]$.

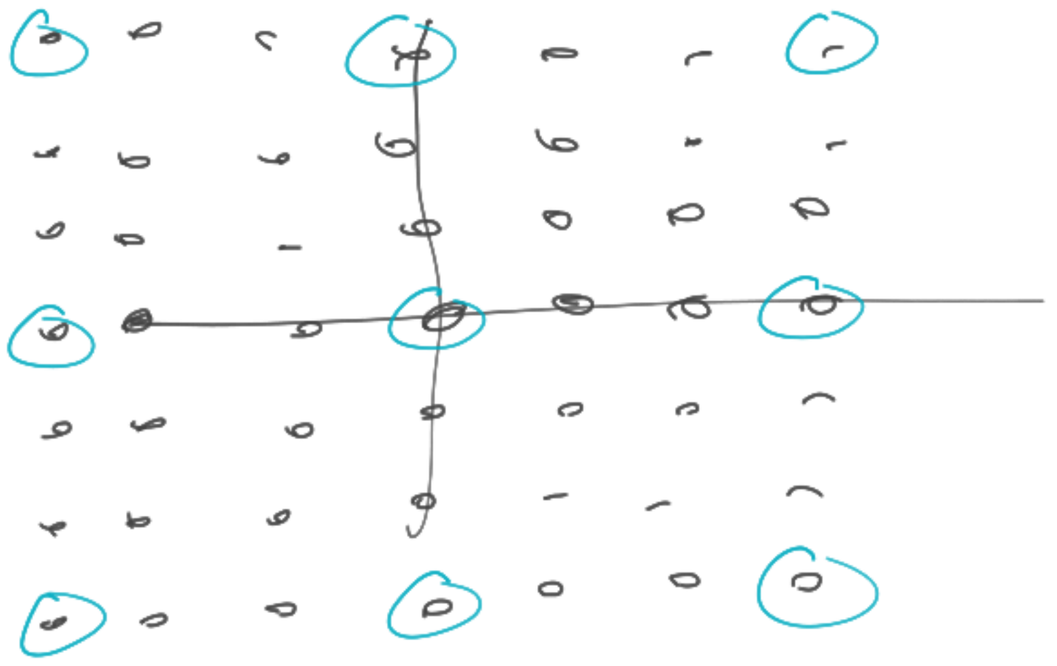
$[i]\cdot[i] = [-1] = [1]$

$[1+i]\cdot[i] = [-1+i] = [1+i]$

$[1+i][1+i] = [2i] = [0]$.

has zero dvs.

$R = \mathbb{Z}[i]$



$I = (3)$

$R/I = \mathbb{Z}[i]/(3)$.

$\cong \mathbb{Z}_3 \times \mathbb{Z}_3$ as additive gp.

Classes: $[a+ib]$ a, b only depend mod 3.

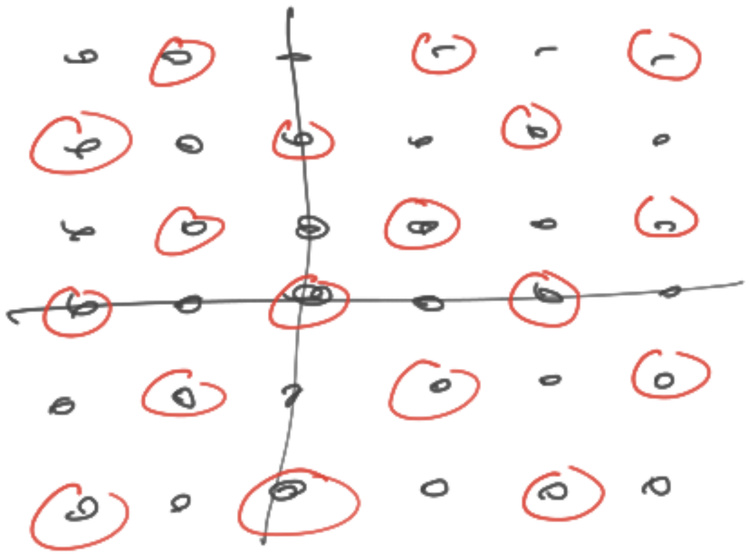
$\Rightarrow$ turns out in this case

$\mathbb{Z}[i]/(3) \cong \mathbb{F}_9$

is a field.

$R = \mathbb{Z}[i]$

$I = (1+i)$



$(1+i) \cdot i = -1 + i$

$-i \cdot (1+i) = 1 - i$

$(1+i) \cdot (1-i) = 2$

$(1+i)(1+i) = 2i$

$$\frac{\mathbb{Z}[i]}{(1+i)} \cong \mathbb{Z}_2 .$$ iso of rings.

$R = \mathcal{C}^\infty(\mathbb{R})$ ring of smooth functions in one variable.

Take any set $X \subseteq \mathbb{R}$.

Consider

$$I_X := \{ f \in \mathcal{C}^\infty(\mathbb{R}) \text{ s.t. } f(x) = 0 \ \forall x \in X \}.$$

$$= \{ \text{smooth functions that vanish along } X \}.$$

it is an ideal:

if $f, g \in I_X$ then $(f+g)(x) = f(x) + g(x)$
$= 0$ if $x \in X$.

if $f \in I_X$ and $g \in \mathcal{C}^\infty(\mathbb{R})$ then $(f \cdot g)(x) = f(x) \cdot g(x)$
$= 0 \cdot g(x) = 0$ if $x \in X$.

$R/I_X \simeq \mathcal{C}^\infty(X)$

In any ring R,

$R \subseteq R$ is an ideal. $R/R \cong$ zero ring.

[if R unital] $R = (1)$.

$(0) \subseteq R$ zero ideal. $R/(0) \cong R$.

Defn: An ideal $I \subseteq R$ is proper if it's neither (0) nor R.

R is simple if it has no proper ideals.

Suppose R unital.

Let u be a unit in R.

If $I \subseteq R$ contains u, then $I = R$

because: if $u \in I$ then $\underbrace{u^{-1}u}_{1} \in I$ ($u^{-1} \in R$)

if $r \in R$ then $\underbrace{r \cdot 1}_{r} \in I$.

if R is a division ring then R is simple.

Conversely, if $a \in R$ is not a unit, then $(a) \neq R$ because $(a) \not\ni 1$.

if R is not a div. ring, then R is not simple.

---

simple + com $\Leftrightarrow$ field.

R commutative r.h.g.

Pick $a \in R$. $\mathrm{Ann}(a)$ annihilator

$\vdots$

$\{x \in R \text{ s.t. } xa = 0\}$.

trivial unless a is a zero div.

ideal: if $xa = 0$ and $ya = 0$

then $(x+y)a = xa + ya = 0$ so additive gp.

if $xa = 0$ and $r \in R$

then $(r \cdot x)a = r(xa) = 0$ so ideal.

Nilradical: $\sqrt{R} := \{a \in R \text{ s.t. } \exists n \text{ s.t. } a^n = 0\}$

= nilpotent elements.

If $a^m = 0$ and $b^n = 0$ then $(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}$

R commutative r.h.g.

Nilradical: $\sqrt{R} := \{a \in R \text{ s.t. } \exists n \text{ s.t. } a^n = 0\}$

= nilpotent elements.

If $a^m = 0$ and $b^n = 0$ then $(a+b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^k b^{m+n-k}$

$$= \sum_{k=0}^{m} \binom{m+n}{k} a^k \underbrace{b^{m+n-k}}_{\geq n \text{ in this sum.}}$$

$$+ \sum_{k=m+1}^{m+n} \binom{m+n}{k} \underbrace{a^k}_{\geq m.} b^{m+n-k}$$

$$= \sum_{k=0}^{n} \left(\; \square \cdot 0 + \sum_{\cdots} (\;) \cdot 0 \right.$$

Arithmetic of ideals:

$I, J \subseteq R$ both ideals

then $I \cdot J := \{ a \cdot b \text{ for } a \in I,\ b \in J \}$.

if $r \in R$ and $a \cdot b \in I \cdot J$

then $r \cdot a \cdot b = (r \cdot a) \cdot b \in I \cdot J$ [absorbing.]

$a \cdot b + a' \cdot b' \overset{?}{\in} I \cdot J$ for $a, a' \in I$, $b, b' \in J$

[closed for addition?]

↑ I still owe you this.

E.g. $(m) \cdot (n) = (m \cdot n)$ for ideals in $\mathbb{Z}$.

Let $I, J \subseteq R$ be ideals.

$$I + J \subseteq R$$

$$\| \quad \{ a+b : a \in I, \ b \in J \}.$$

absorbing? $r \cdot (a+b) = \underbrace{r \cdot a}_{\in I} + \underbrace{r \cdot b}_{\in J} \in I + J.$

closed for addition? $a+b + a'+b' = \underbrace{a+a'}_{\in I} + \underbrace{b+b'}_{\in J}.$

E.g. in $\mathbb{Z}$,

$$(m) + (n) = \{ am + bn : a, b \in \mathbb{Z} \} = (\gcd(m,n))$$

Why ideals?

(1) Kernels of homs. (doesn't explain the name).

(2) Suppose you have a poly, e.g.

$p(x) = x^3 - 2 \in \mathbb{Q}[x]$.

irred in $\mathbb{Q}[x]$. has no roots in $\mathbb{Q}$.

if it did have a root, the root would deserve the name $\sqrt[3]{2}$.

$R = \mathbb{Q}[x]/(p)$ $\ni x + (p) = [x]$ class of x.

$[p] = 0$ in R, and so $[x]^3 = [2]$.

R is a ring in which "$\sqrt[3]{2}$" exists.

(2 cont) ideals ⇝ building rings
in which polynomials have solns.

(3) ideals are all about divisibility.

e.g. (n) = set of nbers div by n.

⇝ way of studying divisibility
in contexts where you may not have
a good thy of factorization.