3/31

- I posted HW #5

Comm Rings w/ 1

$+, \cdot$ $\left(\begin{array}{l} (R,+,0) \text{ abelian group.} \\ (R,\cdot,1) \text{ comm. monoid} \end{array} \right.$

$\cdot$ dist. over $+$.

$(\mathbb{Z}_n, \oplus, \otimes, \bar{0}, \bar{1})$

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

Def. R is an ~~int~~ integral domain if it satisfies the zero divisor property:

$$ab=0 \Rightarrow a=0 \text{ or } b=0.$$

a field $\forall x \neq 0 \ \exists y \ \ xy=1$ ($\Leftrightarrow$ $(R\setminus\{0\}, \cdot, 1)$ is a group.)

Lemma A field is an int. dom.

$P \to (Q \vee R)$

Pf. $ab=0$. $a \neq 0$

P is true, Q is false $\}$ $\to$ R is true

$$b = 1\cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$$

(Let's prove $a \cdot 0 = 0 \ \forall a$. $0+0=0$

$$\underset{+(-a\cdot 0)}{a\cdot 0} = a(0+0) = a\cdot 0 + \underset{+(-a\cdot 0)}{a\cdot 0}$$ left cancel $+$

$$0 = a\cdot 0.$$

(2) R is ~~not~~ an integral domain iff

$\forall a,b,c \ (a\neq 0) \quad ab=ac \Rightarrow b=c$

Pf. $\Rightarrow$ R is an int. dom. + ab = ac

$ab - ac = 0$

$a(b-c) = 0$ int. dom $\Rightarrow b - c = 0$
$\underline{b = c}$.

$\Leftarrow$ WTS R is an int dom

$ab = 0 \quad + \quad a \neq 0$.

$ab = a \cdot 0 =$ canc. $\Rightarrow b = 0$.

Any subring (closed under +, $\cdot$ + contains $\mathbb{1}$) of a field or int. domain is again an int. domain

$\mathbb{Z}$ is ~~not~~ an int. dom., $\mathbb{R}, \mathbb{Q}$, field.

Def. a ring hom. $\varphi: R \to S$. R, S rings.

$$\boxed{\begin{aligned} \varphi(a+b) &= \varphi(a)+\varphi(b) \\ \varphi(ab) &= \varphi(a)\varphi(b) \\ \varphi(1_R) &= 1_S. \end{aligned}}$$

a ring hom is automatically a group hom

$\varphi(0_R) = 0_S$

$\varphi(-a) = -\varphi(a)$

(3) Given a ring hom. $\varphi: R \to S$

$$\operatorname{Ker}\varphi = \{x \in R \mid \varphi(x) = 0_S\}.$$

We know $\operatorname{Ker}\varphi \leq R$ (and normal).

if $a, b \in \operatorname{Ker}\varphi$ then $\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0$.

so it's a subring.

$\operatorname{Ker}\varphi$ has the property that ~~take~~ — absorbtion property

$$\forall a \in \operatorname{Ker}\varphi, \ \forall r \in R, \quad ra \in \operatorname{Ker}\varphi.$$

makes $\operatorname{Ker}\varphi$ into an ideal.

Ex Does $\mathbb{Z} \leq \mathbb{R}$ have this property.

$\pi \in \mathbb{R}$, $2 \in \mathbb{Z}$ $\quad 2\pi \notin \mathbb{Z}$. so $\mathbb{Z}$ does not.

Prop ~~if I is an ideal~~

R is an ideal of R.

$\{0\}$ is an ideal of R.

if I is an ideal of R, and $1 \in I$, then $I = R$. ✓

interested in proper ideals.

(4) $\{$ F is a field. Then the only ideals are $\{0\}$ and F.

Pf. I is an ideal WTS $I = \{0\}$ or $I = F$.

$\{$ $I \neq \{0\}$. $\exists\, x \in I$, $x \neq 0$.

F is a field $x^{-1} \in F$. absorb

$1 = x^{-1} \cdot x \in I$. So $\forall r \in F$

$r = r \cdot 1 \in I$. so $F = I$.

$\boxed{}$

What are the ideals of the integers $\mathbb{Z}$.

remember an ideal is a subring, and a subring is a subgroup.

$\langle n \rangle = n\mathbb{Z} = \{x \mid \exists z \in \mathbb{Z}\ x = n \cdot z\}$

this an ideal. take $x \in n\mathbb{Z}$, take any $y \in \mathbb{Z}$.

$\exists z \in \mathbb{Z}$ $x = n \cdot z$

$y \cdot x = y \cdot n \cdot z = (yz) \cdot n \in n\mathbb{Z}$ $\boxed{}$

(5).

Recall $\{\text{Kernels of a group hom}\} = \{\text{normal subgps.}\}$

gp theory

ring theory $\{\text{Kernels of a ring hom}\} = \{\text{proper ideals.}\}$

I ~~an~~ proper ideal of R $\quad I \subsetneq R \quad 1 \notin I.$

WTS R/I is a ring. we know it's a group ✓ $\quad I \trianglelefteq R$

$(a+I)(b+I) = ab+I.$

show this operation is well-defined. (extra credit)

$\varphi : R \to R/I \qquad r \mapsto r+I$

$\ker\varphi = I$

⑥ Let R, $a \in R$. $\underline{\underline{n\mathbb{Z}}}$

Define $\cancel{aR}$ Ra $= \{x \mid \exists r \in R \; x = r \cdot a\}$.

Prop Ra is an <u>ideal</u> of R.

<u>principal</u> <u>ide~~e~~</u>

<u>princ gen.</u>

$$\boxed{\begin{array}{l}\text{Pf. } r_1 a + r_2 a = (r_1 + r_2) a \\ r(r_1 a) = (r r_1) a\end{array}}$$

$\{0\} = 0 \cdot R$, $R = 1 \cdot R$

~~The~~ $\mathbb{Z}$ has ~~that~~ the property that every ideal is principally gen.

<u>a ring w/ this property has a name.</u>

Principal Ideal Domain aka <u>PID</u>

<u>$\mathbb{Z}$ are a PID</u>

---

if we take a finite set. $a_1, \ldots, a_n$

$\underline{a_1 R + \ldots + a_n R_n} = \{x \mid \exists r_1, \ldots, r_n \in R \;\; x = r_1 a_1 + \ldots + r_n a_n\}$

<u>$\mathbb{Z}$ lin. combination</u>

is an ideal.

7 $x, y \in a_1R + \dots + a_nR = I$

$x = r_1a_1 + \dots + r_na_n \quad r_i \in R$

$y = s_1a_1 + \dots + s_na_n \quad s_i \in R$

$x+y = (r_1+s_1)a_1 + \dots + (r_n+s_n)a_n \in I$

$r \in R$

$rx = r(r_1a_1 + \dots + r_na_n)$

$= (rr_1)a_1 + \dots + (rr_n)a_n \in I.$ $\blacksquare$

An ideal of the form $a_1R + \dots + a_nR_n$ is called a finitely gen. ideal.

prin. gen $\Rightarrow$ f.g.

PID satisfies every ideal is f.g.

A domain satisfying that every ideal is f.g. is called noetherian domain

Example Start w/ a ring and take

$R[x]$ is the set of polynomials w/ coeff from ring R.

a monomial. is a term of the form $\underline{ax^n}$ some $a \in R$
some $n \in \mathbb{N} \cup \{0\}$

a polynomial is of the form

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

we typically assume that $\cancel{}\ a_n \neq 0$.

$\deg f = n$ $\quad a_n$ is called the leading coeff

a_0 is called the constant term

$f(x) + g(x)$ term wise. collect like terms.

$$(ax^n)(bx^m) = ab\,x^{n+m}$$

foil

Ex. $\mathbb{Z}_4$

$$f(x) = 1 + 2x + x^3$$

$2x \cdot 2 = 0$ in $\mathbb{Z}_4$

$$g(x) = 2 + 2x^2$$

$$f(x)g(x) = (1 + 2x + x^3)(2 + 2x^2) = \boxed{2 + 2x^2 + 2x^3 + 2x^5}$$

$$2 + 2x^2 + \underbrace{\cancel{4x} + \cancel{4x^3}}_{=0} + 2x^3 + 2x^5$$

$\mathbb{Z}_4$ $\quad (2x^2)(2x^4) = 0.$ $\qquad \deg(f \cdot g) \neq \deg f + \deg g$

$\mathbb{Z}_4[x]$ not an int. domain.

$\hat{x} = 1 \cdot x^n$

Prop R is an int dom. iff $R[x]$ is an int. dom

iff $\forall f, g \neq 0$ $\deg(fg) = \deg f + \deg g$

x^1

Thm $R[x]$ PID? iff. R is a field

$R[x]$ noetherian domain?

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ $R[x]$

never a domain $R \times S = \{(a,b) \mid a \in R, b \in S\}$ opns coord. wise

$(1,0)(0,1) = (0,0)$

$\varphi : R[x] \to R$ $\varphi(f(x)) = f(0)$ φ is a surj. ring hom.

$\mathbb{Z}[x]$ not a PID $\mathbb{Z}[x_1, x_2, \dots]$ not noetherian

(10)

$\mathbb{R}[x]$ $(x^2+1)\mathbb{R}$ roots x^2+1

$\pm i$

$\mathbb{R}[x] / \underbrace{(x^2+1)\mathbb{R}}_{I}$ $(x+I)^2 = x^2+I = -1+I$

$\cong \mathbb{C}$

Galois Theory