21-373 11/6/2020

Ring Theory! ~ 1860+

Fermat ~ 1650 Diophantus Diophantine?

Easy to show $\forall n \geq 3$ (integer) there are no positive solutions to $a^n + b^n = c^n$.

Most of early Ring Theory was developed to solve this Fermat's last Theorem

Def $(R, +, \cdot, 0)$ is a rng if R non-empty set, $0 \in R$, $+, \cdot$ both binary operations satisfying

(1) $(R, +, 0)$ is abelian group

(2) $(R, \cdot)$ is associative

(3) distributive $\forall a, b, c \in R$,
$a \cdot (b+c) = a \cdot b + a \cdot c$, and
$(b+c) \cdot a = b \cdot a + c \cdot a$

Field $\leq$ Commutative Ring $\leq$ Rng

$\downarrow$ multiplication has an identity

We say R is commutative rng if

- R is a rng
- $\forall a, b \in R$, $a \cdot b = b \cdot a$

R has a unity [= identity] provided $\exists 1_R \in R$ s.t. $(\forall a \in R)$ $a \cdot 1_R = a$ (right unity)
$1_R \cdot a = a$ (left unity)

Example (1) $(\mathbb{Z}, +, \cdot, 0, 1)$ is a commutative rng with 1 as identity

(2) $(2\mathbb{Z}, +, \cdot, 0)$ " without a unity!

(3) $R = \{f : \mathbb{C} \to \mathbb{C}\}$ For all $f, g \in R$, $h(x) = f(x) + g(x)$ $\forall x \in \mathbb{C}$.
$f \cdot g$ is $f(x) \cdot g(x)$ $\forall x \in \mathbb{C}$

(4) $R_1 = \{f : \mathbb{C} \to \mathbb{C} \mid f \text{ is continuous}\}$

(5) $R_2 = \{f : \mathbb{C} \to \mathbb{C} \mid f \text{ is differentiable}\}$

$R_2 \subsetneq R_1 \subsetneq R$

11/5/2020

21-373

Examples of Rings

(1) $(\mathbb{Z}, +, \cdot)$

(2) F is field $\Rightarrow F$ is a commutative ring with identity

(3) $n \geq 2$ $(\mathbb{Z}/n\mathbb{Z}, +, \cdot, 0, 1)$ comm ring with identity

(4) Continuous + differentiable functions
operation: coordinate wise addition

(5) $M_n(F)$ F field – set of $n \times n$ matrices with entries from F is a ring ($n \geq 2$ not commutative)

recall def. field
(A) abelian group +
(M) · assoc
(D) $a \cdot (b+c) = a \cdot b + a \cdot c$

Lemma. Suppose K is a ring,

(Consequence of dist.)
(1) $\forall a \in R$, $a \cdot 0 = 0 \cdot a = 0$ ← identity w.r.t addition!
(2) $\forall a, b \in R$, $(-a)b = -(ab)$

(1) Since $0+0=0 \Rightarrow a(0+0) = a0$

$\overset{\text{dist}}{\Rightarrow}$ $a0 + a \cdot 0 = a \cdot 0$

$a \cdot 0 = 0$

(2) Evaluate $ab + (-a)b = [a + (-a)]b = [0] \cdot b \overset{(1)}{=} 0$

($= ab + (-a)b$ by dist.)

So $(-a)b$ is the inverse (with respect to '+') of ab.

By uniqueness of inverse, $(-a)b = -(ab)$

8f

Most Important Kind of Rings

Polynomial rings. Consider $x^3 + 12x^2 + 19x + 21$.

Add and multiply polynomials get a new ring!

Def. Let R be a commutative ring.

$$R[X] = \{ (a_0, \dots a_n) \mid a_i \in R, n \in \mathbb{N} \}.$$

ring of polynomials in X over R $= \sum_{k=0}^{n} a_k x^k$, $f \in R[x]$; of polynomial

$f = (a_0 \dots a_n)$, $g = (b_0 \dots b_m)$, $m \geq n$

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \dots, a_n + b_n, b_{n+1}, \dots b_m)$$

$$f \cdot g = \sum_{k} c_k x^k = (c_0 \dots, c_n, \dots)$$

where $c_k = \sum_{i=0}^{k} a_{k-i} b_i$ (Cauchy Mult.)

↓ generalization of (normal) expansion of polynomials.

Claim. R commutative $\Rightarrow R[X]$ commutative ring

Remark When F is a field, $F[x]$ is very interesting.

21-373 11/9/2020

Main Result:

The fundamental theorem of arithmetic ($\forall n \geq 2, \exists p_1 < p_2 \dots < p_m$ primes $\exists e_1, e_2 \dots e_m \geq 1$ s.t. $n = \prod_{k=1}^{m} p_k^{e_k}$ and is unique)
can be ~~generated~~ generalized to $F[x]$

(can factorize every polynomial 'uniquely' into 'irreducible polynomials')

$f \in R[x]$

$f = \sum_{k=0}^{n} a_k x^k$. degree of $f = \max\{n \mid a_n \neq 0\}$

How do we generalize integers?

twin primes
$p, p+2$ (e.g. 29, 31)

Def. Let R be a commutative ring with multiplicative identity. $\wedge 1 \neq 0$, $a \in R - \{0\}$ is called a zero divisor if there is $b \in R - \{0\}$ s.t. $a \cdot b = 0$.

R as above is an integral domain iff $\neg \exists a \in R - \{0\}$ zero divisor.

- R commutative
- $\exists 1 \in R - \{0\}$
- $\forall a \forall b \in R - \{0\}, a \cdot b \neq 0$,
  $\iff \neg \exists a, \exists b \in R (a \neq 0 \wedge b \neq 0) \wedge a \cdot b = 0$

Fact. $\mathbb{Z}$ is an integral domain.

Proof. $a \in \mathbb{Z} - \{0\}$, $b \in \mathbb{Z} - \{0\} \Rightarrow a \cdot b \neq 0$

Example $n = p \cdot q$ composite ($p, q \geq 2$) then $\mathbb{Z}/n\mathbb{Z}$ not an integral domain.

Let $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots \overline{n-1}\}$.

$\bar{p}, \bar{q} \in \mathbb{Z}/n\mathbb{Z} \neq \bar{0}$ but $\bar{p} \cdot \bar{q} = \overline{p \cdot q} = \bar{n} = 0$.

e.g. $n = 2 \cdot 5$, $\bar{2} \cdot \bar{5} = \bar{0}$

('Cancellation')

Lemma Suppose R is an integral domain (not necessarily a field!) then

Note that integers don't form a field!

$$\forall\, a \in R - \{0\} \quad a \cdot x = a \cdot y \Rightarrow x = y$$

Proof. $a \cdot x = a \cdot y \Rightarrow a \cdot x - a \cdot y = 0$

$$\Rightarrow a \cdot (x - y) = 0$$

Since $a \neq 0$ and R has no zero divisors,

$$x - y = 0 \Rightarrow x = y.$$

($\mathbb{Z}$ is integral domain but not a field)

Prop Suppose R is a finite integral domain. Then R is a field.

Proof. Want to show existence of inverses.

Given $a \in R - \{0\}$, find $b \in R$ s.t. $a \cdot b = 1$.

Consider $f_a(x) := ax$, $f_a : R \to R$.

By the previous lemma, f_a is injective!

Recall for finite A, $g : A \to A$ is surjective if g is injective.

(Can application of the pigeonhole principle)

false if A is infinite!

If $A = \mathbb{Z}$, $f(x) = 2x$, injective but not surjective

So $\exists\, b \in R$, $f_a(b) = 1 \in R$.

$$a \cdot b = 1$$

Suppose $a \cdot b = 0$ and $a \neq 0$. As $a^{-1} \in F$, multiply by a^{-1}

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

F is a field $\Rightarrow F$ is an integral domain.

Def (Homomorphism)

R_1, R_2 are both rings, $\varphi: R_1 \to R_2$

(1) $\forall a, b \in R_1$, $\varphi(a +_{R_1} b) = \varphi(a) +_{R_2} \varphi(b)$

(2) " $\varphi(a \cdot_{R_1} b) = \varphi(a) \cdot_{R_2} \varphi(b)$

Recall (using group theory)

(1) $\Rightarrow \forall a \in R_1$, $\varphi(-a) = -\varphi(a)$

$\Rightarrow \varphi(0_{R_1}) = 0_{R_2}$.

Def Suppose $\varphi: R_1 \to R_2$ as above. $\ker \varphi = \{a \in R_1 \mid \varphi(a) = 0_{R_2}\}$

Lemma For $\varphi: R_1 \to R_2$ as above, φ is injective $\Leftrightarrow \ker \varphi = \{0_{R_1}\}$

Proof. $\varphi: (R_1, +, 0_{R_1}) \to (R_2, +, 0_{R_2})$ group homomorphism.

($\Rightarrow$) $a \in \ker \varphi \Rightarrow \varphi(a) = 0_{R_2}$. By $\varphi(0_{R_1}) = 0_{R_2}$,

$\varphi(a) = \varphi(0_R) \Rightarrow a = 0_{R_1} \Rightarrow \ker \varphi = \{0_{R_1}\}$

($\Leftarrow$) Let $a, b \in R_1$, suppose $\varphi(a) = \varphi(b)$. $\varphi(a) - \varphi(b) = 0$

$\Rightarrow \varphi(a - b) = 0_{R_2}$

$\Rightarrow a - b \in \ker \varphi$

$a - b = 0_{R_1} \Leftrightarrow a = b$.

Analogues to group theory...

Def. Let R_1, R_2 be rings. We say that R_1 is a subring of R_2 provided

(1) $(R_1, +_1)$ subgroup of $(R_2, +_2)$.

(2) $\forall a, b \in R_1$, $a \cdot_{R_1} b = a \cdot_{R_2} b \in R_1$

[(3) R_1 is also a ring.]

Lemma. Suppose R^* is a ring. If $\{R_i \mid i \in I\}$ all subrings of R^*, then $R := \bigcap_{i \in I} R_i$ is a subring of R^*.

Prop. $\varphi : R_1 \to R_2$ ring homomorphism. Then $\ker R_1$ is a subring of R_1.

- $0_{R_1} \in \ker \varphi$
- $a, b \in \ker \varphi \overset{\text{WTS.}}{\Rightarrow} a - b \in \ker \varphi$.

$$\varphi(a-b) = \varphi(a + (-b)) = \varphi(a) + \varphi(-b) = \varphi(a) - \varphi(b) = 0.$$

$\therefore a - b \in \ker \varphi$.

Closure under multiplication

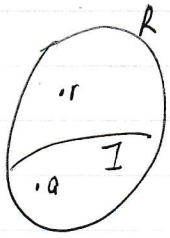
Given $a, b \in \ker \varphi$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = 0 \cdot 0 = 0$, $a \cdot b \in \ker \varphi$.

"abelian" / "normal"

Def. Let R be a rng. $I \subseteq R$ is called ideal provided

(1) $(I,+) \leq (R,+)$

(2) $\forall a \in I$, $\forall r \in R$ we have $r \cdot a \in I$



Recall that if $N \trianglelefteq G$, then $\exists \varphi: G \to G/N$ (natural homomorphism) from G onto G/N

Lemma: If $\varphi: R_1 \to R_2$ ring homomorphism, then $\ker \varphi$ is an ideal.

Proof. (1) ✓ (subring $\Rightarrow$ subgroup)

(2) Given $a \in I$, $r \in R$, enough to show $\varphi(a \cdot r) = 0$.

$$\varphi(a \cdot r) = \varphi(a) \cdot \varphi(r) \underset{a \in \ker \varphi}{=} 0 \cdot \varphi(r) = 0.$$

↑ "Magical" property powered by: transitivity

Lemma Let $(I, <)$ is a linearly ordered set. ($[i < j \wedge j < k \Rightarrow i < k]$, $\forall i,j \in I$, $[i<j \vee i=j \vee j<i]$ comparability, antisymmetry: $a \leq b \wedge b \leq a \Rightarrow a = b$.)

Suppose $\{R_i \mid i \in I\}$ are rings s.t. $i \leq j \Rightarrow R_i$ is subring of R_j.

Then $R^* := \bigcup_{i \in I} R_i$ is a ring and $\forall i \in I$ R_i is a subring of R^*

$H_1, H_2 \leq G$.

$H_1 \cup H_2 \leq G \Leftrightarrow H_1 \leq H_2 \vee H_2 \leq H_1$.

($\Rightarrow$)

21-373 11/13/2020

lemma. Suppose $\{R_i \mid i \in I\}$ are rings s.t. $i<j \Rightarrow R_i$ is subring of R_j.
$\Rightarrow R^* := \bigcup_{i \in I} R_i$ is a ring and $\forall i \in I$, R_i is a subring of R^*.

Proof of lemma. $+, \cdot$ on R^* defined naturally.

(A) $(R^*, +)$ is a group and $(R_i, +_i)$ is a subgroup of $(R^*, +)$

Proof: Given $x, y \in R^*$ $\exists\, i_x, i_y \in I$ s.t. $x \in R_{i_x}$ and $y \in R_{i_y}$.

let $k = \max\{i_x, i_y\}$. Since $i_x \le k$ and $i_y \le k$ by assumption on $\{R_i\}$,

we have R_{i_x} is a subring of R_k and

R_{i_y} " R_k

$\Rightarrow x, y \in R_k$, $x + y = x +_{R_k} y \in R_k$

$\Rightarrow x + y \in R^*$ (since $R_k \subseteq R^*$)

(B) $(R^*, \cdot)$ is closed under multiplication, associative, and distributive w.r.t. '+'.

- Given $x, y, z \in R^*$ take $i_x, i_y, i_z \in I$ s.t. $x \in R_{i_x}$, $y \in R_{i_y}$, $z \in R_{i_z}$.
  $k = \max\{i_x, i_y, i_z\}$. (Each $x, y, z \in R_k$ associative $\Rightarrow R^*$ also associative

- distributivity similar. $x(y+z) = xy + yz$
  $(y+z)x = yx + zx$ $\in R_k$, so it holds also in R^*.

(primary lemma)

lemma 2 and 3 are extensions

Lemma 2. Let $(I, <)$ be a linearly ordered set. Suppose $\{G_i \mid i \in I\}$ are groups such that $i < j \Rightarrow G_i \leq G_j$. Then $G^* := \bigcup_{i \in I} G_i$ has a group structure and $G_i \leq G^*$ $\forall i \in I$. (Similar proof).

Lemma 3. Let R be a given ring. Suppose $(P, <)$ is linearly ordered.
If $\{I_x \mid x \in P\}$ is a family of ideals of R then $I := \bigcup_{x \in P} I_x$ is an ideal of R.
s.t. $x \leq y, I_x \subseteq I_y$

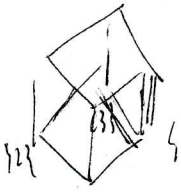
Remark. - When $(P, <)$ l.o. and finite, $\exists\, m \in P$ s.t. $\forall a \in P$, $a \leq m$.
If $\{I_x \mid x \in P\}$ ideals, $I = \bigcup_{x \in P} I_x = I_m$.

- The above lemmas are interesting when the index set is infinite.

Def. $(P, \leq)$ is a partially ordered set if (POSET)
① P is non-empty
② $\leq$ binary relation on P s.t.
- $\forall x \in P,\ x \leq x$
transitivity - $\forall x \forall y \forall z [x \leq y \wedge y \leq z \Rightarrow x \leq z]$
antisymmetry $\forall x \forall y [x \leq y \wedge y \leq x \Rightarrow x = y]$

no connexity! asymmetric

Example (1) $(\mathbb{Z}, <)$ (2) $A = \{1,2,3\}$ $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$
Let $\leq$ be $\subseteq$, $(P, \subseteq)$ is POSET but not linearly ordered!
$\{2\} \not\subseteq \{1,3\}$, $\{1,3\} \not\subseteq \{2\}$.



$\mathcal{P}$-set : 4-dimensional

2(-3)3 11/13/2020

Def. Let $(P, \leq)$ be a POSET. $m \in P$ is called maximal if $\neg\exists a \in P[a \neq m \wedge a \geq m]$.

Remark. In POSET we could have more than 1 max.

In $P = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}\}$ ordered by $\subseteq$ ("throw some elements away")

both $\{1,2\}$ and $\{2,3\}$ are maximal.

Prop. If $(P, \leq)$ POSET and P is finite then $\exists m \in P$ maximal. (prove by induction on size of set.)

Does every POSET (infinite) have a maximal element?

{linear ordered set} $\subseteq$ {POSET}

False. even for linearly-ordered sets! (e.g. $\mathbb{N}, <$).

History

AC (Axiom of Choice). Here

For any family of (non-empty) sets F, there exists a choice function

i.e. $\exists g: F \to \bigcup F$, s.t. $X \in F \Rightarrow g(X) \in X$ $F = \{X, Y\}$, $\bigcup F = X \cup Y$.

(false representation? easy if F is finite, or countable (e.g. get smallest element))

Well-ordering Principle. For every set P there exists $<$ binary relation on P s.t.

$(P, <)$ is linearly ordered and $\forall X \subseteq P, X \neq \emptyset$

$\exists m \in X$, m - minimal (i.e. first)

$\forall a \in P$, $m \leq a$.

When $P = \mathbb{N}$, then $\Leftrightarrow$ Principle of induction.

Clearly when P is countable, (WOP) holds for P.

Interesting when P is uncountable.

1910. E. Zermelo: AC $\Leftrightarrow$ WOP. [21-32 § set theory]

1916. Max Zorn (paper in Proc. of AMS)

"Zorn's Lemma": ZL ① ZL $\Leftrightarrow$ AC

② ZL has several applications to algebra.

Zermelo-Fraenkel

(ZL + ZF $\rightarrow$ WOP/AC)

Kuratowski

21-373 11/16/2020

Given $(P, \leq)$ POSET, is there $m \in P$ maximal?

$[\Leftrightarrow \neg \exists a \in P, a \neq m \wedge a \geq m]$

If P finite, yes.

Else,

Zorn's lemma Let $(P, \leq)$ be a POSET. If for every chain $C \subseteq P$, $\exists b \in P$ upper bound for C, then there exists $m \in P$ maximum.

Def. Let $(P, \leq)$ be POSET.

$\Leftrightarrow \forall x \in C, \forall y \in C [x \leq y \vee y \leq x]$ linear order

Let $b \in P$, $X \subseteq P$. b is an upper bound of X provided $\forall a \in X, a \leq b$.

Def. Let R be a ring, I an ideal of R. I is called maximal (ideal) provided there is no $J \subseteq R$ s.t. $J \supsetneq I$.

Example. Let $R = \mathbb{Z}$, p is prime. $I = p\mathbb{Z}$ is a maximal ideal

Def. Let R, I as above. Suppose R is an integral domain.

I is called prime ideal provided $\forall a, b \in R - \{0\}$, $ab \in I \Rightarrow a \in I \vee b \in I$. (is a multiple of a prime)

Example Then $I = p\mathbb{Z}$ is a prime ideal also.

$\Updownarrow$

(Euclid's lemma) Let $a, b \in \mathbb{Z}$, p prime.

$p \mid ab \rightarrow p \mid a \vee p \mid b$.

Generalization of prime numbers!

(e.g. $3\mathbb{Z}$, $5\mathbb{Z}$ ...)

Remark. Let $R=\mathbb{Z}$. In R, I is maximal $\Leftrightarrow$ I is prime ideal.

Theorem I max $\Rightarrow$ I prime (but converse is generally not true)

Suppose R is a field. What are the ideals of R?

- $\{0\}$ is an ideal
- R is an ideal

Find $\{0\} \subsetneq I \subsetneq R$ ideal? Not possible.

Lemma. If R is a field, $I \neq \{0\}$ ideal, then $I=R$.

Proof. Since $I \neq \{0\}$, $\exists a \in I$, $a \neq 0$. R is a field $\Rightarrow \exists b \in R$, $b \cdot a = 1$.
As I ideal, $b \cdot a \in I \Rightarrow 1 \in I$. But I closed under multiplication,
So $\forall r \in R$, $r \cdot 1 \in I \Rightarrow r \in I \Rightarrow R \subseteq I$.

What are the ideals of $\mathbb{Z}$? $\{n\mathbb{Z} \mid n \in \mathbb{Z}\}$

$6\mathbb{Z}$, $4\mathbb{Z}$ are not prime ideals.

Remark $6\mathbb{Z}$ cannot be a maximal ideal. $6\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$
$6\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$.

Given a ring R, we can always find a maximal ideal. Use Zorn, start from $\{0\}$

Example. Let I be an infinite set, F a field.
$R = F[\{x_i \mid i \in I\}]$. ring of polynomials with coefficients in F. $P \in R \Leftrightarrow \exists i_1, \dots i_n \in I$ s.t. $P \in F[x_{i_1}, \dots x_{i_n}]$

Need to show $\forall J \subsetneq R$ ideal, $\exists J^* \subsetneq R$ max ideal s.t. $J^* \supseteq J$.

Theorem Suppose R has identity 1. If $J \subsetneq R$ ideal, then there exists (given) $J^* \supseteq J$ maximal ideal of R.

Proof. Consider $\mathcal{P} := \{I \subseteq R \mid I \text{ ideal}, 1 \notin I, I \supseteq J\}$ (could be just $\{J\}$)

$(\mathcal{P}, \subseteq)$ (inclusion) is a POSET. Note that $M \subsetneq R$ ideal is maximal iff $M \in \mathcal{P}$ is max.

We can use Zorn's lemma to complete the proof once we show

$\mathcal{C} \subseteq \mathcal{P}$ is a chain $\Rightarrow \exists b \in \mathcal{P}$ upper bound.

Suppose $\mathcal{C} \subseteq \mathcal{P}$ is a chain.

Let $I := \bigcup \mathcal{C}$.

Claim: $I \in \mathcal{P}$ and I is an upper bound of $\mathcal{C}$

Proof: As $1 \notin C_k \; \forall C_k \in \mathcal{C}$, $1 \notin I$.

I is an ideal: proved on Pg 94!

Given $x, y \in I$, $\exists I_1, I_2 \in \mathcal{C}$, $x \in I_1, y \in I_2$.

WLOG, $I_1 \subseteq I_2$: $x, y \in I_2 \Rightarrow x - y \in I_2 \subseteq I$.

For $r \in R$, $r \cdot x \in I_1 \subseteq I$, $r \cdot y \in I_2 \subseteq I$

$\therefore I \supseteq J$. (every J can be extended)

Given $C_k \in \mathcal{C}$, by def of union, $C_k \subseteq \bigcup \mathcal{C} = I$.

Then by Zorn's lemma, there exists a maximal ideal in R.

Zorn's lemma has further Applications: Every finite vector space has a basis

21-373 11/18/2020

For ring with identity $1 \neq 0$

$I \subsetneq R$ is prime ideal if $\forall a,b \in R$, $ab \in I \to a \in I \vee b \in I$

$I \subsetneq R$ is maximal ideal if $\forall$ ideal $J \subsetneq R$, $J \supseteq I \to J = I$

Theorem (Zorn's Lemma)

R is with $1 \neq 0$. Then $\forall I \subsetneq R$ ideal, $\exists I^* \supseteq I$ maximal.

Example. $\forall p$ prime : $p\mathbb{Z}$ is both a prime ideal and a maximal ideal.

(2) $\{0\}$ is a prime ideal of $\mathbb{Z}$, but not maximal ideal.
This is because $\forall n \geq 2$, $\{0\} \subsetneq n\mathbb{Z} \subsetneq \mathbb{Z}$.

Recall . $N \trianglelefteq G$, $G/N = \{aN : a \in G\}$ is a group, with $(aN)\cdot(bN) \overset{\text{def}}{=} (ab)N$.

. $\varphi : G \to G/N$ the natural homomorphism $\varphi(a) = aN$ is a surjective homomorphism.

. First Isomorphism. $\varphi : G \to H$ surjective homomorphism $\Rightarrow H \cong G/\ker\varphi$.
$G \to \varphi(G)$ is always surjective, so we obtain the same results.

Let $\varphi : R_1 \to R_2$ be ring homomorphism, then

Fact. $\ker\varphi = \{a \in R_1 \mid \varphi(a) = 0_{R_2}\}$ is an ideal. $0_{R/I} = 0 + I$

Def. Suppose $I \subseteq R$ ideal, $R/I = \{a + I : a \in R\}$

$$(a+I) \oplus (b+I) := (a+b)+I$$
$$(a+I) \odot (b+I) := (ab)+I$$

Theorem. $(R/I, \oplus, \odot)$ is a ring, $\varphi : R \to R/I$ given, $\varphi(a) = a+I$ is a surjective ring homomorphism.

Need We only need to prove distributivity.

21373 11/18/2020

Dist. Evaluate $(a+I)\odot((b+I)\oplus(c+I)) \overset{\text{def}\oplus}{=} (a+I)\cdot((b+c)+I)$

$\overset{\text{def}\odot}{=} a(b+c)+I$

$\overset{R \text{ distributive}}{=} (ab+ac)I$

$\overset{\text{def of}\oplus}{=} (ab+I)\oplus(ac+I)$

$\overset{\text{def}\odot}{=} [(a+I)\cdot(b+I)]\oplus[(a+I)\cdot(c+I)]$

Theorem Let R be commutative, with identity $1\neq 0$. Suppose $I \subsetneq R$ is ideal.
I is prime $\Leftrightarrow$ R/I is an integral domain.

if I not prime, e.g. $\mathbb{Z}$, $\bar{2}\cdot\bar{3}=\bar{0}$!

~~Corollary If R is commutative, $1\neq 0$, $I \subsetneq R$ and R/I is a field, then I is prime.~~

(this means if $\mathbb{Z}/n\mathbb{Z}$ is a field, then n is prime).

Lemma Suppose R has $1\neq 0$. $I \subseteq R$ ideal. Then I is proper $\Leftrightarrow$ $1\notin I$.

Suppose I proper, but $1\in I$. Then by second property of ideals,
$\forall r\in R,\ r\cdot 1 \in I \Rightarrow r\in I\ \forall r\in R$
$\Rightarrow I = R$, not proper!

if $1\notin I$ clearly $I \subsetneq R$ since $1\in R$.

Def $u\in R$ is **unit** provided $\exists v\in R$ s.t. $u\cdot v = 1$, R commutative.

Example. (i) If R is a field, then $\forall u\in R-\{0\}$ is a unit

(ii) In $\mathbb{Z}$ the only units are 1 and -1.

not necessary to have $1 \in I$!

Lemma* Let $I \subseteq R$ ideal. If $\exists\, u \in I$ unit, then $I = R$.

By the second property of ideals, $\forall r \in R$, $r \cdot u \in I$, take $v \in R$ s.t. $u \cdot v = 1$, $u \cdot v = 1 \in I \Rightarrow 1 \in I \Rightarrow I = R$. (last theorem)

(aside) left ideal → closure by left multiplication.
right ideal → closure by right multiplication
} in commutative rings these are the same
two-sided ideal → left + right ideal

$R = F[x]$, $I = \{\sum_{i=1}^{n} a_i x^i \mid a_i \in F, n \in \mathbb{N}\}$, proper ideal of R.
$= xF[x]$ (no constant coefficient term!)

(Proof of Theorem!) Let R be commutative ring with $1 \neq 0$. $I \subsetneq R$ ideal
I is prime $\Leftrightarrow$ R/I is an integral domain

($\Rightarrow$) Suppose R/I is not integral domain. $\exists (a+I), (b+I) \in R/I$ not zero, which means $[a+I \neq I$ and $b+I \neq I]$ (written $\wedge$) $(a+I) \odot (b+I) = I$.

$0_{R/I} = I = 0+I$

Fact. $H \leq G$, $a \in G$, $a \in H \Leftrightarrow a \cdot H = H$ $[aH = H \subseteq G \cdot H]$

$a \notin I$, $b \notin I$

$ab + I = I$ (def)

$\therefore ab \notin I$.

So we found $a, b \in R$ s.t. $ab \in I$ but $a \notin I \wedge b \notin I \Rightarrow I$ is not prime.

($\Leftarrow$) Suppose R/I integral domain, I not prime. $\exists a, b \in R$ s.t. $ab \in I$ but $a \notin I \wedge b \notin I$, $a \notin I \Rightarrow a+I \neq I$, $b \notin I \Rightarrow b+I \neq I$. So $a+I$ and $b+I$ are non-zero elements of R/I. Since we have $ab+I = I$, def $\odot \Rightarrow (a+I) \odot (b+I) = I \Rightarrow (a+I) \odot (b+I) = 0_{R/I}$. So R/I not integral domain!

Recall R commutative, $1 \neq 0$, I ideal, I is prime $\Leftrightarrow$ R/I integral domain.

11/20/2020

21-373

To prove:

I is maximal $\Leftrightarrow$ R/I field (field is integral domain; $\Rightarrow$ I maximal must be prime).

$\{0\}$ is prime, but not maximal in $\mathbb{Z}$.

$\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\}$ not field!

Def R ring, I ideal.

R/I field $\Rightarrow$ I is prime

I is prime $\not\Rightarrow$ R/I field

$(a+I) \oplus_{R/I} (b+I) \overset{\text{def.}}{:=} a+b+I$

$(a+I) \odot_{R/I} (b+I) := ab+I$

Lemma Let R, I be as above. $\varphi: R \to R/I$ given by $\varphi(a) = a+I$ is a ring homomorphism

$\to$ (natural / canonical) homo.

(Proof) From Group Theory, as $(I,+) \trianglelefteq (R,+)$, $\varphi: (R,+) \to (R/I, \oplus)$ is a surjective homomorphism.

φ is a ring homomorphism: Enough to show, for $a, b \in R$,

$\varphi(a \cdot b) = \varphi(a) \odot_{R/I} \varphi(b)$.

If $\varphi(a) \odot \varphi(b) = (a+I) \odot (b+I) \overset{\text{def } \odot}{=} ab+I \overset{\text{def}(\varphi)}{=} \varphi(a \cdot b)$

special case

Theorem (First Isomorphism) Suppose $\varphi: R_1 \to R_2$ surj ring homomorphism, then

$R_2 \cong R_1/\ker\varphi$ (as rings)

$\bar{\varphi}: R_1/\ker\varphi \xrightarrow{\cong} R_2$ given by $\bar{\varphi}(a+\ker\varphi) = \varphi(a)$, $\bar{\varphi}$ bijective!

Need to check $\bar{\varphi}\left((a+I) \odot (b+I)\right) \overset{?}{=} \varphi(a) \cdot \varphi(b)$.

Lemma R is a field $\Leftrightarrow$ R has only trivial ideals
(no ideal such that $\{0\} \subsetneq I \subsetneq R$)

Proof. ($\Rightarrow$)
For sake of contradiction, suppose $\exists\, I \subsetneq R$ ideal, $I \neq \{0\}$
Take $a \in I$, $a \neq 0$. As R is a field, $\exists\, b \in R$, $b \cdot a = 1$.
By 2nd property of ideals, $ba \in I \Rightarrow 1 \in I \overset{\text{2nd prop}}{\Rightarrow} r \cdot 1 \in I \ \forall r \in R$
$\Rightarrow I = R$.

($\Leftarrow$) Let $a \in R - \{0\}$.

"cyclic subgroup"? 'minimal'

Consider $I = \{r \cdot a \mid r \in R\}$

Claim: I is an ideal of R.

Proof. Clearly $0 \in I$ since $0 = 0 \cdot a$.

Lagrange (subgroup) Given $r_1, r_2 \in R$, $r_1 - r_2 a = (r_1 - r_2) a \in I$
($r_1 - r_2 \in R$)

Given $b \in R$, $ra \in I$, $b(ra) = \underbrace{br}_{r_1}(a) = \in I$ ☐ claim.

Since $a \in I$ ($1 \in R$, $1 \cdot a \in I$), $a \neq 0$, we have $I \neq \{0\}$.

By assumption on R, necessarily $I = R$.

Since $1 \in R$, we have $1 \in I \Rightarrow \exists\, r_1 \in R$ s.t. $1 = r_1 a$.

So r_1 is an inverse of a.

Lemma. Let R_1, R_2 be rings. Suppose $\varphi: R_1 \to R_2$ surjective homomorphism.

(a) If $I \subseteq R_1$ ideal, then $\varphi[I]$ ideal of R_2.

(b) If $J \subseteq R_2$ " $\varphi^{-1}[J]$ " R_1.

this theorem holds for other substructures e.g. vector subspace $x=y$ in R^2. subfields...

Proof. Since $0_{R_1} \in I$, as $0_{R_2} = \varphi(0_{R_1}) \in \varphi[I]$ (so $\varphi[I]$ not empty)

→ Given $a, b \in \varphi[I]$, let $a', b' \in I$ s.t. $a = \varphi(a'), b = \varphi(b')$

$a - b = \varphi(a') - \varphi(b') = \varphi(a'-b') = \varphi(c') \in \varphi[I]$.

(φ homo of group)

→ Given $r \in R_2$, $a \in \varphi[I]$, let $r' \in R_1$, $a' \in I$ be such that

$\varphi(r') = r$, $\varphi(a') = a$

$r \cdot a = \varphi(r')\varphi(a') = \varphi(r'a') = \varphi(b) \in \varphi(I)$

(φ homo; I ideal; $r'a' \in I$.)

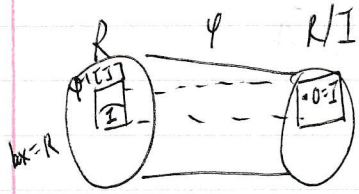
(b) Exercise.

Proof of main theorem (finally!) | let R be commutative, with $1 \neq 0$. Suppose $I \subsetneq R$ ideal. I is a max ideal of $R \iff R/I$ is a field.

non-commutative ring: $n \times n$ matrix not commutative, not inverse!

Fix $\varphi: R \to R/I$ natural (surjective) homo. $\varphi(a) = a + I$.

($\Rightarrow$) to show that $\nexists J$ proper ideal of R/I. (s.t. $J \neq \{0_{R/I}\}$)



otherwise, suppose $I \subsetneq J \subsetneq R/I$.

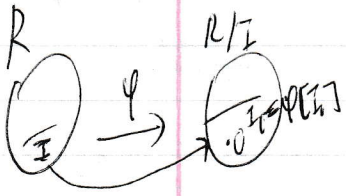
Then $\varphi^{-1}[J]$ ideal of R.

Since $I \subsetneq J$, $\varphi^{-1}[J] \supsetneq I$, we found an ideal of R properly containing I!

Since I is max, we have $\varphi^{-1}[J] = R$. $1 \in \varphi^{-1}[J] \Rightarrow 1 \in J$, $J = R/I$. ↯

($\Leftarrow$) W.T.S R/I is field $\Rightarrow$ I is a maximal ideal of R.

Suppose R/I field, and I not maximal.



let $J_1 \trianglelefteq_R$ ideal such that $J_1 \supsetneq I$. Consider $I_1 := \varphi[J_1]$.

By the homomorphism lemma, $\varphi[J_1]$ ideal of R/I.

Since $0_{R/I} = I$ and $J_1 \supsetneq I$, $I_1 \supsetneq \{0\}$.

As R/I is a field, we have $I_1 = R/I$

So $1_{R/I} \in I_1 \Rightarrow 1 \in J_1 \Rightarrow J_1 = R$.

Important concepts, $1 \in I$ causes the ideal to expand

a commutative ring (non-field) must have non-trivial ideals.

In group theory, we considered $(A \leq G)$ $\langle A \rangle$ the subgroup generated by A

$$A := \bigcap_{H \leq G,\, H \supseteq A} H$$

Special case $A = \{c\}$, $\langle c \rangle$ the cyclic group generated by $A = \{c^n \mid n \in \mathbb{Z}\}$.

A more constructive definition is $\langle A \rangle = \{a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \mid n \in \mathbb{N}, a_i \in A, \varepsilon_i \in \{1, -1\}\}$

$A \subseteq R$. $\langle A \rangle$ the subring generated by A!

(A) ideal generated by A.

$\bigcap J$ (J ideal of R, $J \supseteq a$.)

Lemma Let R be a commutative ring with $1 \neq 0$.

Then R is a field $\Leftrightarrow$ The ideals of R are $\{0\}$ and R.
(R has no non-trivial ideals)

Proof ($\Rightarrow$) $I \subseteq R$ ideal, $I \supsetneq \{0\} \Rightarrow \exists\, a \in R-\{0\}$. R field $\Rightarrow \exists\, b \in R$ $ba = 1$.

I is closed under multiplication by elements of $R \Rightarrow 1 \in I \Rightarrow \forall a \in R$, $a \cdot 1 \in I$

$\therefore a \in I$.

($\Leftarrow$) Take $a \in R-\{0\}$, we need to show $\exists\, b \in R$ s.t. $b \cdot a = 1$.

Consider $I = \{r \cdot a \mid r \in R\}$. Then we claimed I is an ideal...

$a \neq 0$ & $a = 1 \cdot a \in I \Rightarrow I \supsetneq \{0\}$.

By assumption, $R = I$. As $1 \in R$, $1 \in I$, By definition of I,

$1 \in I \Rightarrow (\exists\, r \in R)$ $r \cdot a = 1$. so we have found the inverse of every a!

Def. Suppose R is an ideal, $A \subseteq R$.

$$(A) := \bigcap_{\substack{J \text{ ideal of } R \\ J \supseteq A}} J$$ ← the ideal generated by A. ($\simeq$ subgroup generated by subset)

Remark. When $A = \{a\}$, $a \in R$, $(A) := I$ (in the previous proof).

Claim: let $a \in R$ ($1 \in R$), $(a) = \overline{\{r \cdot a \mid r \in R\}}^{I}$ (ideal generated by a)

Pf. note that I is an ideal: $r_1 a - r_2 a = (r_1 - r_2)a = r_3 a \in I$, clearly $0 = 0 \cdot a \in I$

$s(ra) = (sr)a = r'a \in I$.

Since $1 \in R$, $a = 1 \cdot a \in I$.

So I is an ideal containing a. Thus as (a) is the smallest ideal of R containing a,

$(a) \subseteq I$

Now want to show $I \subseteq (a)$.

If $b \in I$, then $\exists r \in R$ s.t. $b = r \cdot a$.

As (a) is an ideal, for any $r \in R$ and $x \in (a)$,

$r \cdot x \in (a)$. As $a \in (a)$, $r \cdot a \in (a)$

$\Rightarrow b \in (a)$

$\therefore b \in I \Rightarrow b \in (a)$

Theorem. Suppose R has $1 \neq 0$. $A \subseteq R$.

$$(A) = \{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R, n \in \mathbb{N}, a_i \in A \}.$$ (I)

Remark. The last claim is a special case of this theorem.

$(a_i = a)$, RHS $= \{r \cdot a \mid r \in R\}$.

Proof. (WTS $(A) \subseteq I$) As $1 \in R$, clearly $A \subseteq I$ (Since $\forall a \in A$, $a = 1 \cdot a \in I$)

Subclaim: I is an ideal. Proof: Given $\sum r_i a_i, \sum s_j h_j \in I$,

then there are $t_i \in R, c_i \in A$, $\sum r_i a_i - \sum s_j h_j = \sum t_i c_i \in I$

Given $r \in R$ and $\sum r_i a_i \in I$,

$r(\sum r_i a_i) = \sum (r \cdot r_i) a_i = \sum r_i' a_i \in I$. ($r_i' = r \cdot r_i$)

As I is an ideal containing A, by definition of (A), clearly $(A) \subseteq I$.

(WTS $I \subseteq (A)$) Given $\sum_{i=1}^{n} r_i a_i \in I$, as $a_i \in (A)$ and (A) ideal, we have $r_i \cdot a_i \in (a)$ for all $1 \leq i \leq n$

As (a) closed under $+$, $\sum r_i a_i \in (a)$.

So $x \in I \Rightarrow x \in (A)$ ✓

21-373 11/23/2020

Now think of $\mathbb{Z}$ and $\mathbb{Q}$. $\mathbb{Q} = \{\frac{a}{b} \mid a,b \in \mathbb{Z}, b \neq 0\}$

$\mathbb{Z}$: integral domain; $\mathbb{Q}$: field

$\mathbb{Q}$ "inherits" $\mathbb{Z}$. (OOP!) e.g. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

How to construct $\mathbb{Q}$ from $\mathbb{Z}$?

Multiplicative Group of Integers Modulo n.

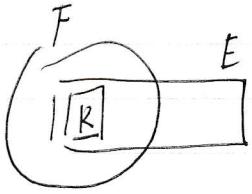
e.g. n=7

0
1 ✓
2 ✗
3 ✓ generator! $\varphi(6)=2$
4 ✗
5 ✓ 4 6 2 3 1
6 ✗ ±1

excl. 0, $\mathbb{Z}/7\mathbb{Z}^{\times}$ is cyclic with generators 3 and 5

Theorem If R is an integral domain [R is commutative, $1 \neq 0$, has no zero divisors] (for $a \neq 0$, $ax=ay \Rightarrow x=y$)

then there exists a field F s.t. R is subring of F, and if E is a field s.t. R is a subring of E, then $\exists\, \varphi: F \to E$ field homomorphism, with $\varphi|_R = id_R$



"F is the field generated by R"

Field of fractions

(Let $R = \mathbb{Z}$, $F = \mathbb{Q}$)

First - field homomorphisms: $\varphi: R_1 \to R_2$ ring homomorphism $\Rightarrow$ $\varphi(x \pm y) = \varphi(x) \pm \varphi(y)$ (1)

$\varphi(0) = 0$ (2)

when R_1 and R_2 have identities, we need a more "specialized" definition:

$\varphi: R_1 \to R_2$ ring homomorphism for rings with 1_{R_1}, 1_{R_2},

we need (1) + (2) + (3): $\varphi(1_{R_1}) = 1_{R_2}$

Recall from Group Theory. $\varphi: G_1 \to G_2$ ($\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \Rightarrow \varphi(1_{G_1}) = 1_{G_2}, \varphi(a^{-1}) = \varphi(a)^{-1}$)

However, for rings this must be explicitly checked!

Theorem: Suppose E, F are fields. If $\varphi: F \to E$ is ring homomorphism, then φ is injective.

"preserve information!"

Proof. Use Facts: ① $\ker \varphi$ is an ideal. (also, F has only trivial ideals)

② $\ker \varphi = \{0\} \iff \varphi$ is injective.

Enough to show $\ker \varphi = \{0\}$. Since $\varphi(1_F) = 1_E \neq 0_E$

↑ axiom of field!

$\therefore 1_F \notin \ker \varphi. \Rightarrow \ker \varphi \neq F$

$\Rightarrow \ker \varphi = \{0\}$

N.B. $\varphi(1_{F_1}) = \varphi(1_{F_2})$ automatically because multiplication is a group.

Q7. $|G| = p^n \Rightarrow \exists\, N \trianglelefteq G,\ |N| = p$.

Th 1 $|G| = p^n \Rightarrow |Z(G)| \geq p$

Th 2 (Cauchy) If p prime, $p \mid |G| \Rightarrow \exists\, a \in G,\ |\langle a \rangle| = p$.

Using Theorem 1, $Z(G)$ not trivial, Lagrange $p \mid |Z(G)| \overset{\text{Th 2}}{\Rightarrow} \exists\, a \in Z(G),\ |\langle a \rangle| = p$

Trivial to show that $H \leq Z(G) \Rightarrow H \trianglelefteq G$. ($H$)

Theorem: R is an integral domain [$\equiv 1 \in R - \{0\}$, R has no zero divisors] then there exists a field F_R such that R is a subring of F_R ~~def~~.

- Furthermore, if E is a field s.t. R is a subring of E then $\exists\, \varphi : F_R \to E$ homomorphism s.t. $\varphi \upharpoonright R$ (restriction of domain to R) $= id_R$. ($f \upharpoonright C = \{(x,y) \in f \mid x \in C\}$ rest)
- Def. F_R called the field of fractions of R

$\forall a \in R,\ \varphi(a) = a$.

Example: $R = (\mathbb{Z}, +, \cdot)$, $F_R = \mathbb{Q}$

If E is a field s.t. R is subring of E, find $\varphi: \overset{(F_R)}{\mathbb{Q}} \to E$.

$$\varphi\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)} = \frac{\varphi(a)}{1} = \frac{a}{1} = a$$

($\uparrow \in R := \frac{a}{1}$)

Proof. Let $S = R - \{0\}$. Consider $A = \{(x,y) \mid x \in R, y \in S\}$.

Define $(x,y) \sim (x_1, y_1) \overset{\text{def.}}{\Leftrightarrow} xy_1 = x_1 y$: binary relation on A.

Easy to show that this is an equivalence relation (Symm ✓ Refl ✓ Trans ✓)

set of equivalence classes $F_R := \{[(x,y)] \mid (x,y) \in A\}$ $\quad [(2,1)] = [(6,3)] = [(20,10)] \ldots$

Idea: when $x \in \mathbb{Z}$, $y \in \mathbb{Z} - \{0\}$, $[(x,y)]$ is $\frac{x}{y}$. $(= xy^{-1})$.

Now we define

$$\oplus : [(x,y)] \oplus [(x_1,y_1)] := [(xy_1+yx_1, y\cdot y_1)]$$

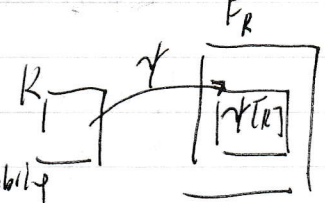
$$\odot : [(x,y)] \odot [(x_1,y_1)] := [(xx_1, yy_1)]$$

tedious to check well-definedness and $(F_R, \oplus, \odot)$ is a field.

$x, y \in S \Rightarrow x \cdot y \in S$ $\quad 1_{F_R} = [(1,1)]$, $0_{F_R} = [(0,1)]$

Consider $\varphi : R \to F_R$ given by $\varphi(a) = [(a,1)]$

φ is an injective ring homomorphism!



"cut and paste"

Identify R with $\varphi[R]$ by renaming the subring as $\varphi[R]$ of F_R. We have R is a subring of F_R.

Last part ("~~uniqueness~~ uniqueness") Given E field s.t. R is a subring of E, find $\psi : F_R \to E$ homomorphism s.t. $\forall a \in R, \psi(a) = a$.

$a \in R$, $b \in R - \{0\}$, find $\psi([(a,b)])$:

$\psi([(a,b)]) := \frac{a}{b}$ according to E

$a \in R$, a represented by $[(a,1)]$,

$\psi([(a,1)]) := \frac{a}{1} = a \Rightarrow \psi(a) = a$.

21-373 12/2/2020

$F[X]$ – ring of polynomials with coefficients from F field. (also works for $R[X]$, for R integral domain)

Check $F[X]$ is an integral domain: Given $p, q \in F[X]$,

$$\deg(p \cdot q) = (\deg p) + (\deg q)$$

($\sum_{k=0}^{n} a_k X^k \quad \sum_{k=0}^{m} b_k X^k$, the leading coefficient of $p \cdot q$ is $a_n b_m$

Since $a_n \neq 0, b_m \neq 0 \Rightarrow a_n \cdot b_m \neq 0$.

Let p prime, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, Consider $R = \mathbb{F}_p[X]$. (p prime)

Applying the theorem, $F_R = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{F}_p[X], g \neq 0 \right\} = \mathbb{F}_p(X)$ field of fractions of R.

Note: every finite field has prime power order

Case $p=2$, $\mathbb{F}_2 = \{0, 1\}$, but $\mathbb{F}_2(X)$ is infinite, containing $\{X^n \mid n \in \mathbb{N}\}$.

X^2+1
X^3+1

[$\forall a \in \mathbb{F}_2(X)$, $a + a = 0$
so $\mathbb{F}_2$ has characteristic 2]

Def. Recall that if I ideal of R, we say I is generated by a provided.

$I = (a) := \{r \cdot a \mid r \in R\}$.

For I ideal of R, I is called <u>principal</u> provided $\exists a \in I$, s.t. $I = (a)$.

R is called <u>principal ideal domain (PID)</u> provided:

(1) R is an integral domain
and (2) Every ideal is principal.

Ex. (1) $\mathbb{Z}$ every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z} := (n)$. All subgroups of $\mathbb{Z}$ we called ...

(2) F field $\Rightarrow F[X]$ is a PID

Midterm 2 Scribbles

integral domain:
$a(x-y)=0 \Rightarrow x=y$

Finite Integral Domain → Field

Given $x \neq 0$ find x^{-1}

$f(a) = ax$ → show function is injective!

$a_1 x = a_2 x \Rightarrow (a_1 - a_2)x = 0$

$\Rightarrow a_1 = a_2$

since R is finite, f is also surjective.

$\exists\, a$ s.t. $ax = 1$

$\therefore a = x^{-1}$.

$H \leq G$

WTS $G \neq \bigcup_{g \in G} gHg^{-1}$

Consider the action of G on subsets of G by conjugation

$orbit(H) = \{ gHg^{-1} \mid g \in G \}$, $|orbit(H)| = [G : G_H] = \frac{|G|}{|N_G(H)|} = m$

$G_H := \{ g \in G \mid gHg^{-1} = H \}$

$= N_G(H)$

Sec 7.6 (CRT)

$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$

$\left| \bigcup_{g \in G} gHg^{-1} \right| \leq (|H|-1)\frac{|G|}{m} + 1$

$\leq (|H|-1)\frac{|G|}{|H|} + 1$

$\leq |G| - \frac{|G|}{|H|} + 1$

$\leq |G| - 2 + 1 < |G|$.

Midterm 2 Q1:

$p^n \quad m$

eg. $p=5, m=3$

$n=4$

$p^2 \times m$

$p^3 \times m$

group action = multiply by p mod mp^n

{1, 5, 7, 75, 375, ...}

{10, 50, 250, 1250, ...}

$p^3 \times p^3 \times m =$

want to show $\binom{mp^n}{p^n} \equiv m \bmod p$.

$G = \mathbb{Z}/p^n\mathbb{Z}$, $B = \{1, 2, 3, \ldots, m\}$

$|S| = |X|$, where $X = \{x \subseteq G \times B \mid |x| = p^n\}$

$= \binom{mp^n}{p^n}$

reduction!

21-373 12/4/2020

R is Principal Ideal Domain (PID) $\Leftrightarrow$ (1) R is commutative, $1 \neq 0 \in R$, R has no zero divisors (an integral domain), and (2) for any ideal $I \subseteq R$, $\exists i \in I$, $(i) = I$ (where $(i) = \{r \cdot i \mid r \in R\}$)

[Examples. (a) $\mathbb{Z}$ is a PID (b) F field, $F[x]$ PID]

Def. Let R be an integral domain, $a, b \in R - \{0\}$. $d \in R$ is a greatest common divisor of a and b (not unique!) provided

(1) $d \mid a \wedge d \mid b$

(2) If $d' \mid a \wedge d' \mid b$ then $d' \mid d$

$a \mid b \Leftrightarrow (\exists r \in R)\ b = r \cdot a$

(we could explicitly define 'greatest' because R could be finite and there could be no order)

(return x, y s.t. $ax+by = \gcd(a,b)$)

```
gcd(a,b):
  if b<a return gcd(a,b)
  if b==1: return(0,1)
  (x,y) = gcd(b, a mod b)
  return (y, x - y⌊a/b⌋)
```

(use Euclid's algorithm for gcd, when $R = \mathbb{Z}$.)

(Bézout's theorem: $\gcd(a,b) = ax + by$ and $\gcd(b, a \bmod b) = \gcd(a,b)$)

Let R be a PID. $\forall a, b \in R - \{0\}$, $\exists d \in R$, s.t. d is a gcd of a and b. Moreover, $\exists x, y \in R$ s.t. $d = ax + by$.

Proof. Consider $I := \{ax + by \mid x, y \in R\}$.

Check that I is an ideal of R, $= (\{a, b\})$

As R is PID, $\exists d \in I$, $(d) = I$.

Let $x_0, y_0 \in R$, s.t. $d = ax_0 + by_0$.

(the gcd is a 'generator')

Claim: d is a gcd of a and b.

Pf: (1) Show $d \mid a \wedge d \mid b$.

Take $x = 1$ & $y = 0$. $ax + by \in I \Rightarrow a \cdot 1 + b \cdot 0 = a \in I$.

$x = 0$ & $y = 1$. $\Rightarrow a \cdot 0 + b \cdot 1 = b \in I$.

Since $(d) = I$, $\exists r_a \in R$ s.t. $a = r_a d$

$\exists r_b \in R$ s.t. $b = r_b d$.

(2) If $d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$.

$\exists r_a, r_b \in R$, $a = r_a d'$, $b = r_b d'$. Since $d = ax_0 + by_0 = (r_a d')x_0 + (r_b d')y_0$

$= d'(r_a x_0 + r_b y_0)$

$= d' r \Rightarrow d' \mid d$ //

Recall

def Suppose R is an integral domain, $u \in R - \{0\}$ is called a unit provided $\exists\, v \in R - \{0\}$ s.t. $u \cdot v = 1$.

Example: In $\mathbb{Z}$, both 1 and -1 are units. In $F[x]$, the units are the elements of $F - \{0\}$. If $f(x)g(x) = 1$.

Then $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) = 0$.

$\therefore \deg(f(x)) = \deg(g(x)) = 0$.

Lemma Let R be an integral domain, $a, b \in R - \{0\}$.

If $(a) = (b)$ then $\exists\, u \in R$ s.t. $a = u \cdot b$.

$(\exists\, v \neq u \cdot v = 1,\ v \cdot a = b.)$

Proof. Since $(a) = (b)$, as $a \in (a)$ we have $a \in (b) \therefore \exists\, r_a \in R,\ a = r_a b$.

$b \in (a) \Rightarrow \exists\, r_b \in R,\ b = r_b a$.

$a = r_a(r_b a) \Rightarrow a = (r_a r_b)a$

$\Rightarrow 1 \cdot a = r_a r_b\, a$.

Since R is integral domain, can "cancel" $1 = r_a r_b$, r_a, r_b both units.

Take $u := r_a$.

Recall (1) $I \subsetneq$ ideal is maximal $\Leftrightarrow \neg\exists J$ ideal, $[I \subsetneq J \subsetneq R]$ "cannot squeeze in"

(2) R int domain, $I \subsetneq R$ is prime $\Leftrightarrow \forall a, b,\ a \cdot b \in I \Rightarrow a \in I \vee b \in I$.

Theorem. For R comm, $1 \neq 0$,

(1) I maximal $\Leftrightarrow R/I$ field

(2) I prime $\Leftrightarrow R/I$ integral domain

$\Rightarrow$ I maximal $\Rightarrow$ I prime

Special case. In $\mathbb{Z}$, we have $n\mathbb{Z}$ is maximal $(\Leftrightarrow) n\mathbb{Z}$ is prime

(n is a prime number)

Theorem Let R be a PID, $I \subsetneq R$ ideal.

I is prime $\Leftrightarrow$ I is maximal

Pf. ($\Leftarrow$) by previous corollary

($\Rightarrow$) Suppose I is prime. Since R is PID, $\exists p \in I$ s.t. $(p) = I$.
Given an ideal J s.t. $I \subseteq J \subseteq R$, to show that I is maximal
enough to show either $J = I$ or $J = R$.

As R is PID, $\exists j \in J$ s.t. $(j) = J$. Since $p \in I \subseteq J = (j)$

$\Rightarrow \exists r \in R,\ p = r \cdot j$.

$rj \in (p) \Rightarrow r \in (p) \vee j \in (p)$
(I is prime)

$(\exists x \in R,\ r = xp$ (a) or $\exists y \in R,\ j = yp$ (b)$)$

If (a) So $p = (xp)j \Rightarrow p = p(xj) \Rightarrow xj = 1$
$\Rightarrow j$ unit $\Rightarrow 1 \in (j)$.
$\Rightarrow (j) = R$

If (b) $(j) \subseteq (p)$, but $(p) = I \therefore (j) \subseteq I$
$\Rightarrow J = I$

- Gödel nobody
- Euclid fundamentals
- Theorem of Arithmetic
- → Identify 'primes'

textbook defines 'irreducibles' to be 'not a unit'

for next time...

Def. Let R be an integral domain, $a \in R - \{0\}$ Euclid's lemma

(1) a is called prime iff (a) is prime ideal. [$a \mid xy \Rightarrow a \mid x \vee a \mid y$]
($xy \in (a) \Rightarrow x \in (a)$ or $y \in (a)$)

(2) a is irreducible iff $\exists x, y \in R$ s.t. $a = xy \Rightarrow x$ unit or y unit.
(or -1 if $R = \mathbb{Z}$)

Theorem Let R be a PID, $p \in R - \{0\}$, p is prime $\Leftrightarrow$ p is irreducible.

12/7/2020

I is prime $\Leftrightarrow \forall a,b \in R \; ab \in I \Rightarrow a \in I \vee b \in I$

I is max $\Leftrightarrow \nexists J$ ideal , $I \subsetneq J \subsetneq R$

Fact I max $\Rightarrow I$ is prime
(Assuming R is an integral domain)

Theorem: R is PID $\Leftrightarrow R$ integral domain and $\forall I \subseteq R$ ideal $\Rightarrow \exists\, i \in I$ s.t. $(i) = I$
(I is principal)

Def. Let R be an integral domain, $r \in R - \{0\}$.

(1) r is prime $\Leftrightarrow (r)$ is prime. ($u \in R-\{0\}$ unit $\Leftrightarrow \exists\, v \in R,\ u \cdot v = 1$)
(2) r is irreducible $\Leftrightarrow \forall a,b \in R,\ r = a \cdot b \rightarrow a$ unit or b unit

Theorem. Let R be a PID, $p \in R - \{0\}$. Then p is irreducible $\Leftrightarrow p$ is prime.

Pf. ($\Rightarrow$) Enough to show that (p) is maximal (maximal ideal $\Rightarrow$ prime ideal). Let $I = (p)$.

Let $J \subseteq R$ be ideal s.t. $J \supseteq I$ (WTS $J = I \vee J = R$)

Since R is PID, $\exists\, j \in J$, $(j) = J$.

Since $p \in (p) = I \subseteq J = (j)$, so $p \in (j) \Rightarrow (\exists\, r \in R)\ p = r \cdot j$.

Since p is irreducible, either

r is a unit $\Downarrow$ $p = rj \Rightarrow r'p = r'rj = j$. $\therefore j \in (p) = I$ $\Downarrow$ $J = (j) \subseteq I$ $\Downarrow$ $J = I$.

or j is a unit. $\Downarrow$ ($u \in I \Rightarrow I = R$) $\exists\, j' \in R,\ j \cdot j' = 1$. So $j \in J \Rightarrow 1 \in J$ $\Rightarrow J = R$

So $I = (p)$ is maximal.
($\Rightarrow I$ is a prime ideal)

[We use only R is integral domain]

($\Leftarrow$) $ab \in (p) \Rightarrow a \in (p) \vee b \in (p)$

let $a, b \in R - \{0\}$ s.t. $p = a \cdot b \in (p) \overset{\text{prime}}{\Rightarrow} a \in (p) \vee b \in (p)$

$\exists r_1 \in R,\ a = r_1 p$

Since $ab = p$,

$1 \cdot p = p = ab = (r_1 p) b = r_1 b p$

Since R is an integral domain,

$r_1 b = 1$.

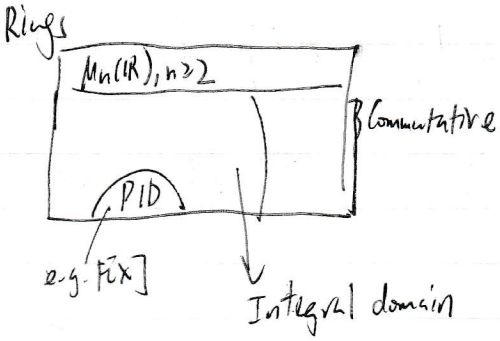
$\therefore b$ is unit.

$\exists r_2 \in R,\ b = r_2 p$

$a(r_2 p) = ab = p$.

$a r_2 = 1$.

$\therefore a$ is unit.



* A field is a PID. Only ideals are 0 and F itself.

Fundamental objects in (1) Algebraic Number Theory
(2) Algebraic Geometry

Abstract Algebra (A brief History)

Galois 1830s

Cauchy 1870s

Dedekind Ring Theory ($\sim$ 1880)

Fermat's $a^n + b^n = c^n$ ($n \geq 3$?)

Emmy Noether (1920-1932)

(post docs) + Emil Artin

+ B.L van der Waerden

- Algebraic structures as sets with operations!

PID $\subsetneq$ UFD $\subsetneq$ Integral domain

Def Let R be an integral domain. R is called a **Unique Factorization Domain** (UFD) if $\forall r \in R - \{0\} \cup \text{Unit}(R))$,

$\exists \langle p_1, \dots p_n \rangle$ all irreducible, s.t.

sequence - could be repeating

existence (1) $r = \prod_{k=1}^{n} p_k$ (in $\mathbb{Z}$: prime factorization, without using exponentiation notation)

uniqueness (2) if $\langle q_1, \dots q_m \rangle$ all irreducible s.t. $r = \prod_{l=1}^{m} q_l$

then $n=m$ and $\exists \sigma \in S_n$ s.t. $p_i \sim q_{\sigma(i)}$, $\forall i \in \{1, \dots n\}$.

$15 = 3 \cdot 5$
$= (-3)\cdot(-5)$

When $p \sim q$ ('associates') $\Leftrightarrow$ $(\exists u \in \text{unit}(R))$ $p = u \cdot q$.

Remark: $\sim$ eq relation [$p \sim q \Leftrightarrow p$ and q are associates]

Goal: **Theorem** R is UFD $\Rightarrow$ R is PID. ($\Leftarrow$ Fundamental Theorem of Algebra when $R = \mathbb{Z}$ is PID)

Theorem: Suppose R is UFD, $p \in R - \{0\}$. p is irreducible $\Leftrightarrow$ p prime.

(prime $\Rightarrow$ irreducible follows from previous, since $R \in$ UFD $\Rightarrow$ R is integral domain)

($\Rightarrow$) Suppose p is irreducible. WTS (p) is prime ideal.

Take $a, b \in R - \{0\}$ s.t. $a \cdot b \in (p)$.

$\exists r \in R$ s.t. $ab = r \cdot p$.

As R UFD, factor both a and b as product of irreducibles.

$$\underbrace{(\prod p_i)}_{a}\ \underbrace{(\prod q_j)}_{b} = r \cdot p.$$

By the uniqueness part, $p \sim p_i$ or $\exists j\ p \sim q_j$

$p \mid a \Rightarrow a \in (p)$ $\quad p \mid b \Rightarrow b \in (p)$.

For R integral domain,

R UFD $\Leftrightarrow \forall r \in R - \{0\}$. Existence $\exists p_1, p_2 \cdots p_n$ irreducible, u unit, such that $r = u \cdot p_1 p_2 \cdots p_n$

Uniqueness if $r = v \cdot q_1 \cdots q_m$ also irreducible, v unit, then $n = m$ and $\exists \sigma \in S_n$, $p_i \sim q_{\sigma(i)}$ $\forall i$

($p \sim q \Leftrightarrow \exists$ unit u, $p = uq$)

Fact. ① If R PID, p is irreducible $\Leftrightarrow$ p is prime $\quad 6 = 2 \cdot 3 = -3 \cdot -2$ (etc.)

② If p is irreducible (= prime for PIDs), then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ (Euclid's lemma)

③ ① and ② hold for UFD.

Main Theorem. If R is a PID, then R is a UFD. (Cor. Fundamental Theorem of Arithmetic — every integer has a prime factorization)

Proof. Existence for sake of contradiction, $\exists r \in R - \{0\}$ non-unit that can't be written as product of irreducibles (primes)

- r can't be irreducible (else $1 \cdot r$)
- So r is not irreducible $\Rightarrow \exists r_0, r_1 \in R - \{0\}$, $r = r_0 \cdot r_1$, at least one of $\{r_0, r_1\}$ is irreducible.

- take smallest positive integer without factorization (w.o.p) if a prime ✓ else — break down (but theorem both have factors!)
- Difficulty is that there's no ordering in arbitrary rings)

$r = r_0 \cdot r_1$

r_{00} r_{01} r_{10} r_{11}

r_{110} r_{111}

r_{1110} r_{1111}

Suppose r_1 is not irreducible. $\exists\ r_0, r_1 \in R - \{0\}$ s.t. $r_1 = r_{10} r_{11}$

(If both r_0 // r_{11} are irreducible, then r_1 is a product of irreducibles.)

Otherwise, r_0 not irreducible and not a product of irreducibles. So $r_0 = r_{00} r_{01}$

Suppose r_{11} not irreducible, then $r_{11} = r_{110} \cdot r_{111}$

As $r = r_{00} \cdot r_{01} \cdot r_{10} \cdot r_{110} \cdot r_{111}$ by assumption that r is not product of irreducibles

By induction, $\forall n \in \mathbb{N}$ find $r_{11\ldots1\ldots1}$ ($n+1$ ones), $r_{11\ldots10}$ (n ones) s.t.

$$r_{11\ldots1} = r_{11\ldots1} \cdot r_{11\ldots10}$$

(n ones) ($n+1$ ones) (n ones)

if $r_1 = r_2 b$

$r_2 = r_1 c$

$\Rightarrow b \cdot c = 1$

Define $I_n = (r_{11\ldots1})$ (n times). Since $r_{11\ldots1}$ ($n+1$ ones) $\mid r_{11\ldots1}$ (n ones),

we have $I_n \subseteq I_{n+1}$ (I_n particular $I_n \subsetneq I_{n+1}$)

- we don't assume R is countable!
- if R finite, finite integral domain is field, and every element is a unit!

Fact. If $\{ I_n \subseteq R \mid n \in \mathbb{N} \}$ ideals s.t. $I_n \subseteq I_{n+1}\ \forall n$, then

$I = \bigcup_n I_n$ is an ideal. ~~Note that~~

* Note that as R is PID, $\exists\ a \in I$, $(a) = I \Rightarrow \exists n \in \mathbb{N}, a \in I_n$.

$\Rightarrow I_n \supseteq (a) = I$.

$\Rightarrow I_n = I_{n+1}$

Contradiction!

21-373 12/9/2020

Uniqueness

Suppose $r = u \cdot p_1 \cdots p_n$, $p_1 \cdots p_n$ not necessarily distinct but all irreducible

$r = v \cdot q_1 \cdots q_m$, $q_1 \cdots q_m$ "

WLOG, $n \le m$. Argue by induction on n:

$n=1$ $r = u p_1 = v q_1 \cdots q_m$

Since p_1 is irreducible (p is irreducible $\Rightarrow p$ is prime $\Rightarrow p \mid ab \Rightarrow p \mid a \vee p \mid b$)

So $\exists i$, $p_1 \mid q_i$. As q_i is irreducible, $\exists u_1$ unit s.t.

$q_i = u_1 p_i$

As R is integral domain, we can cancel!

$u = v' q_1 \cdots \cancel{q_i} \; q_{i+1} \cdots q_m$

ok, no need to do anything else since this is already a unit

General case. $u p_1 \cdots p_n = v q_1 \cdots q_m$.

p287. Again by Euclid's lemma, $u p_2 \cdots p_n = v q_1 \cdots q_{j-1} q_{j+1} \cdots q_m$

then apply the inductive hypothesis

assume that p_1 divides q_j.

(which follows from)