1/14/2014

Welcome Back.

Recall

(1) Math 661.
Noncommutative Algebra DONE.
Groups & Representations
Intro to "Lie Theory".

(2) Math 662
Commutative Algebra
Rings & Fields
Intro to "Algebraic Geometry"

The subject is based on an analogy between

$\mathbb{Z}$ $K[x]$

The Integers Polynomials in 1 variable over a field

Number Theory $\longleftrightarrow$ Geometry.

The course will be in two parts:

(A) Study of $\mathbb{Z}$ and $K[x]$

- Jordan Canonical form
- modules over a PID
- Galois Theory (see MTH 562)

(B) Study of $\mathbb{Z}[y]$ and $K[x,y]$

- Introduction to Algebraic Geometry.

But first, some Philosophy.

Let S, T be sets and let $R \subseteq S \times T$ be a relation. We will write

$$aRb \iff (a,b) \in R$$

Given a subset $A \subseteq S$ we define

$$A^* := \{ t \in T : aRt \ \forall a \in A \} \subseteq T$$

and similarly for $B \subseteq T$ we define

$$B^* := \{ s \in S : sRb \ \forall \ b \in B \} \subseteq S.$$

This gives us a pair of maps

$$* : 2^S \to 2^T$$
$$* : 2^T \to 2^S$$

called an abstract Galois connection.

Let's explore the basic properties.

(1) $*$ is order-reversing. That is, given $A_1, A_2 \subseteq S$ with $A_1 \subseteq A_2$ we have

$$A_2^* \subseteq A_1^*$$

Proof: Assume that $A_1 \subseteq A_2 \subseteq S$ and consider any $t \in A_2^* \subseteq T$. By definition this means that

$$aRt \quad \forall \ a \in A_2$$

But since $A_1 \in A_2$ this implies that

$$aRt \quad \forall \quad a \in A_1.$$

Hence $t \in A_1^*$ ///

Now consider the compositions

$$** : 2^S \to 2^S$$
$$** : 2^T \to 2^T$$

(Sorry for the abuse of notation.)

(2) $**$ is monotone increasing. That is, for all $A \subseteq S$ we have

$$A \subseteq A^{**}$$

Proof: Given $a \in A$ we want to show that $a \in A^{**}$. Recall that

$$A^{**} = (A^*)^* = \{ s \in S : sRt \ \forall \ t \in A^* \}$$

So we want to show that

$$aRt \ \forall \ t \in A^*.$$

So consider any $t \in A^*$. By definition this means that sRt $\forall$ $s \in A$, and in particular we have aRt.

Since this is true for any $t \in A^*$ we have

$$aRt \quad \forall \quad t \in A^*,$$

as desired. //

(3) For all $A \subseteq S$ we have

$$A^{***} = A^*.$$

Proof: Consider any $A \subseteq S$. By (2) we have $A \subseteq A^{**}$. Then applying (1) gives

$$A^{***} = (A^{**})^* \subseteq A^*.$$

Conversely, applying (2) to the set $A^* \subseteq T$ gives

$$A^* \subseteq (A^*)^{**} = A^{***}.$$ //

Now we discuss the notion of "closure"

Def: Given a set U we say that $cl: 2^U \to 2^U$ is a closure operator if it satisfies

i) $\forall X \subseteq U, \quad X \subseteq cl(X)$

ii) $\forall X, Y \subseteq U, \; X \subseteq Y \Rightarrow cl(X) \subseteq cl(Y)$

iii) $\forall X \subseteq U, \; cl(cl(X)) = cl(X)$.

We say that the set $X \subseteq U$ is closed if

$$cl(X) = X.$$ ///

(4) $**$ is a closure operator.

Proof: i) Given $A \subseteq S$, part (2) says that $A \subseteq A^{**}$ ✓

ii) Given $A_1, A_2 \subseteq S$ with $A_1 \subseteq A_2$, we apply part (1) twice to get

$$A_1 \subseteq A_2 \Rightarrow A_2^* \subseteq A_1^* \Rightarrow A_1^{**} \subseteq A_2^{**}$$ ✓

iii) Given $A \subseteq S$ we apply (3) to get

$$(A^{**})^{**} = (A^{***})^{*}$$
$$= (A^{*})^{*} = A^{**}$$

as desired. ///

(5) The $**$-closed subsets of S form a lattice with

$$1 = S, \quad 0 = T^{*}, \quad \wedge = \cap.$$

Proof: Note that S is closed because.

$$S \subseteq S^{**} \implies S^{**} = S.$$

Note that T^{*} is closed because

$$(T^{*})^{**} = T^{***} = T^{*} \text{ by } (3).$$

Furthermore, if $A \subseteq S$ is closed then we have $T^{*} \subseteq A$ because

$$A^{*} \subseteq T \implies T \subseteq A^{**} = A \text{ by } (1).$$

Finally suppose that $A_1, A_2 \subseteq S$ are closed. We will show that $A_1 \cap A_2$ is also closed.

Indeed, applying (1) gives

$$A_1 \cap A_2 \subseteq A_1 \Longrightarrow (A_1 \cap A_2)^{**} \subseteq A_1^{**} = A_1$$

$$A_1 \cap A_2 \subseteq A_2 \Longrightarrow (A_1 \cap A_2)^{**} \subseteq A_2^{**} = A_2$$

It follows that $(A_1 \cap A_2)^{**} \subseteq A_1 \cap A_2$ and we conclude that

$$(A_1 \cap A_2)^{**} = A_1 \cap A_2 .$$

The join operation is

$$A_1 \vee A_2 = \bigcap_{A_1 \cup A_2 \subseteq X \subseteq S} X$$

X is closed.

//

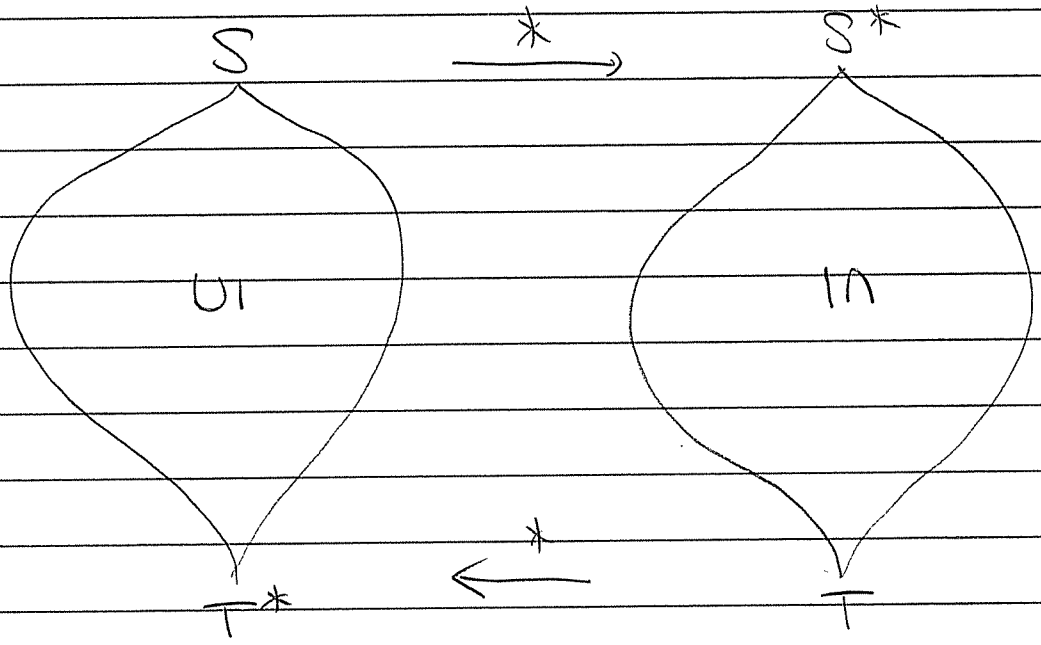
Finally we have a theorem.

Theorem (Abstract Nonsense):

The maps $*: 2^S \to 2^T$

$*: 2^T \to 2^S$

are inverse and order-reversing bijections between the lattices of $**$-closed sets



Proof: If $A \subseteq S$ is closed then part (3) implies that

$$A^* = A^{***} = (A^*)^{**},$$

hence $A^* \subseteq T$ is also closed. Thus $*: 2^S \to 2^T$ and similarly $*: 2^T \to 2^S$ send closed sets to closed sets. They are inverses when restricted to closed sets because if $A^{**} = A$ then

$$(A^*)^* = A^{**} = A.$$

What does that have to do with anything?

Both sections of the course

(A) $\mathbb{Z}$ and $K[x]$

(B) $\mathbb{Z}[y]$ and $K[x,y]$

Center around an abstract Galois correspondence

(A) Centers on Galois' (~1820) Galois correspondence

and

(B) Centers on Hilbert's (~1890) Nullstellensatz ("zero places theorem").

To be continued...

1/16/14

I'll assign HW 1 next Tues
I'm out of town next Thurs

Recall the plan for MTH 662

(A) $\mathbb{Z}$ and $K[x]$

(B) $\mathbb{Z}[y]$ and $K[x,y]$.

We will begin by discussing unique factorization in rings.

BEGIN

Definition: A ring is a structure $(R, +, \times, 0, 1)$ such that

- $(R, +, 0)$ is an abelian group.
- $(R, \times, 1)$ is an abelian semigroup
- $\forall a, b, c \in R$ we have

$$a(b+c) = ab + ac.$$ ///

[Do we want to say $0 \neq 1$?]

We say that $S \subseteq R$ is a subring if

- $0_R, 1_R \in S$
- $(S, +_R, \times_R, 0_R, 1_R)$ is a ring. ///

Given a ring R, let

$$R^\times := \{a \in R : \exists\, b \in R,\ ab = 1\}.$$

Note that $(R^\times, \times, 1)$ is a group, called the group of units. ///

A field is a ring K in which

$$K^\times = K - \{0\}.$$

A domain is a subring of a field.

The Prototype:

$$\mathbb{Z} \subseteq \mathbb{Q}$$

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

Note that a domain $R \subseteq K$ satisfies

$$a, b \neq 0 \implies ab \neq 0.$$

Proof: We will show that

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

So suppose that $ab = 0$ and $a \neq 0$. Note that $a \in R \subseteq K$ has an inverse $a^{-1} \in K$. Hence in K we have

$$\begin{aligned} ab &= 0 \\ a^{-1}ab &= a^{-1}0 \\ b &= 0. \end{aligned}$$

This also holds in R. ///

Conversely, suppose that R is a ring in which

$$a, b \neq 0 \implies ab \neq 0.$$

Does it follow that R is a subring of a field?

How could we find such a field?

Consider the set of abstract symbols

$$\mathrm{Frac}(R) := \left\{ \left[\frac{a}{b}\right] : a, b \in R,\ b \neq 0 \right\}$$

where we declare

$$\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right] \iff ad = bc.$$

This is an equivalence because if

$$\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right] \quad \text{and} \quad \left[\frac{c}{d}\right] = \left[\frac{e}{f}\right]$$

then we also have $\left[\frac{a}{b}\right] = \left[\frac{e}{f}\right]$.

Indeed, we have

$$ad = bc.$$
$$adf = b(cf)$$
$$adf = b(de).$$
$$d(af - be) = 0$$

Since $d \neq 0$ and R is a domain, this implies

$$af - be = 0 \Rightarrow af = be \Rightarrow \left[\frac{a}{b}\right] = \left[\frac{e}{f}\right].$$

Now consider $\left[\frac{a}{b}\right]$ and $\left[\frac{c}{d}\right] \in Frac(R)$. Since $b \neq 0$ and $d \neq 0 \Rightarrow bd \neq 0$, it makes sense to declare

$$\left[\frac{a}{b}\right]\left[\frac{c}{d}\right] := \left[\frac{ac}{bd}\right]$$

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] := \left[\frac{ad + bc}{bd}\right]$$

But we should check that this is well-defined.

Check $\times$: If $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$ and $\left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right]$ then

$$\begin{aligned}(ac)(b'd') &= (ab')(cd') \\ &= (ba')(dc') \\ &= (bd)(a'c').\end{aligned}$$

$$\Rightarrow \left[\frac{ac}{bd}\right] = \left[\frac{a'c'}{b'd'}\right].$$

Check +: If $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$ and $\left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right]$ then

$$\begin{aligned}(ad+bc)(b'd') &= (ad)(b'd') + (bc)(b'd') \\ &= (ab')(dd') + (cd')(bb') \\ &= (ba')(dd') + (dc')(bb') \\ &= (bd)(a'd') + (bd)(b'c') \\ &= (bd)(a'd' + b'c')\end{aligned}$$

$$\Rightarrow \left[\frac{ad+bc}{bd}\right] = \left[\frac{a'd'+b'c'}{b'd'}\right] \quad ///$$

One can check that Frac(R) is a ring with

$$0_{Frac(R)} = \left[\frac{0_R}{1_R}\right]$$

$$1_{Frac(R)} = \left[\frac{1_R}{1_R}\right]$$

In fact, Frac(R) is a field.
Indeed, we have

$$\left[\frac{a}{b}\right] \neq \left[\frac{0}{1}\right] \Rightarrow a1 \neq b0$$
$$a \neq 0$$

Thus $\left[\frac{b}{a}\right]$ is defined and we have

$$\left[\frac{a}{b}\right]\left[\frac{b}{a}\right] = \left[\frac{ab}{ba}\right] = \left[\frac{1}{1}\right] = 1_{\mathrm{Frac}(R)}$$

because $ab1 = ba1$. ///

Finally note that the elements

$$\left\{\left[\frac{a}{1}\right] : a \in R\right\}$$

form a subring of $\mathrm{Frac}(R)$ isomorphic to R.

Formally, we say that a map of rings $\varphi : R \to S$ is a <u>ring homomorphism</u> if

- $\forall\, a, b \in R,\ \varphi(a+b) = \varphi(a) + \varphi(b)$
- $\forall\, a, b \in R,\ \varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_S$.
  (This is NOT automatic.)

Then the map

$$R \hookrightarrow \mathrm{Frac}(R)$$
$$a \longmapsto \left[\frac{a}{1}\right]$$

is an injective ring homomorphism.

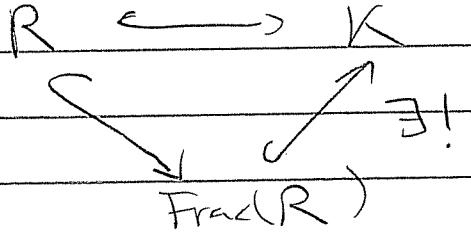
In summary, we have the following.

Theorem: Let R be a ring. Then we have

$$\forall\, a, b \in R,\ a, b \neq 0 \Rightarrow ab \neq 0$$

if and only if $\exists$ a field K and an injective ring map $R \hookrightarrow K$.

This field is not unique, but there is a minimal such field called the field of fractions $\mathrm{Frac}(R)$.



Note that there are many rings with the same field of fractions.

For example, consider the ring

$$\mathbb{Z}\left[\tfrac{1}{2}\right] = \left\{ a_0 + a_1\left(\tfrac{1}{2}\right) + \cdots + a_n\left(\tfrac{1}{2}\right)^n : a_i \in \mathbb{Z} \right\}$$

$$= \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b = 2^n \right\}$$

called the ring of dyadic rationals.

Clearly

$$\mathbb{Z} \subsetneq \mathbb{Z}\left[\tfrac{1}{2}\right] \subsetneq \mathbb{Q}$$

But we have

$$\mathrm{Frac}(\mathbb{Z}) = \mathrm{Frac}\left(\mathbb{Z}\left[\tfrac{1}{2}\right]\right) = \mathbb{Q}.$$

More generally, given any subset $0 \notin S \subseteq \mathbb{Z}$ that is closed under multiplication, we define

$$\mathbb{Z}[S^{-1}] = \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ b \in S \right\}$$

This is called the localization of $\mathbb{Z}$ by S.

Note that

$$\text{Frac}(\mathbb{Z}[S^{-1}]) = \mathbb{Q}$$

and if $S = \mathbb{Z} - \{0\}$ then we have

$$\mathbb{Z}[S^{-1}] = \mathbb{Q}$$

Given a domain R, the localizations interpolate between R and its field of fractions

$$R \subseteq R[S^{-1}] \subseteq \text{Frac}(R)$$

1/21/14

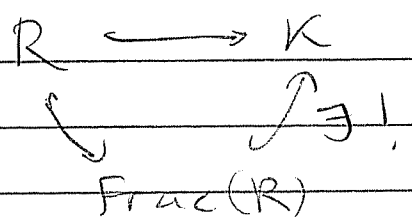
HW 1 is due Tues Feb 4.

NO CLASS THIS THURSDAY

We have a webpage!

Office Hours: Mon 2-3, Wed 3-4.

Last time we discussed the field of fractions of a domain R. It has the universal property that if K is a field and $R \hookrightarrow K$ is an injection then there exists a unique injection $\mathrm{Frac}(R) \hookrightarrow K$ such that



More generally, given any subset $S \subseteq R$ such that

- $0 \notin S$
- $1 \in S$
- $a, b \in S \Rightarrow ab \in S$

we can define the localization of R by S:

$$R[S^{-1}] = \left\{ \frac{a}{b} : a, b \in R,\ b \in S \right\}$$

Note that we have

$$R \subseteq R[S^{-1}] \subseteq \mathrm{Frac}(R)$$

and $\mathrm{Frac}(R[S^{-1}]) = \mathrm{Frac}(R)$
for any such S.

Most generally, let R be any ring and consider $S \subseteq R$ such that

- $1 \in S$
- $a, b \in S \Rightarrow ab \in S$

(S is a subsemigroup of $(R, \times, 1)$).

Then we can define the localization

$$R[S^{-1}] := \left\{ \frac{a}{b} : a, b \in R,\ b \in S \right\}$$

with

$$\frac{a}{b} = \frac{c}{d} \iff \exists \text{ unit } u \in R \text{ such that } uad = bc.$$

(See HW 1.3)

Soon we will see the geometric interpretation of localization...

Today: Isomorphism Theorems

Given rings R, S we say that a function $\varphi: R \to S$ is a ring map (or a ring homomorphism) if

- $\varphi(a+b) = \varphi(a) + \varphi(b) \quad \forall a, b \in R$
- $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in R$
- $\varphi(1_R) = 1_S$

We define

$$\operatorname{im}\varphi = \{\varphi(a) : a \in R\} \subseteq S$$
$$\ker\varphi = \{a \in R : \varphi(a) = 0_S\} \subseteq R.$$

Note that the image is a subring of S. Indeed, we have $0_S, 1_S \in \operatorname{im}\varphi$ because

$$0_S = \varphi(0_R) \quad \text{and} \quad 1_S = \varphi(1_R).$$

Then for all $\varphi(a), \varphi(b) \in \operatorname{im}\varphi$ we have

$$\varphi(a) + \varphi(b) = \varphi(a+b)$$

hence $\varphi(a) + \varphi(b) \in \operatorname{im}\varphi$ and

$$\varphi(a)\varphi(b) = \varphi(ab)$$

hence $\varphi(a)\varphi(b) \in \operatorname{im}\varphi$. ///

Q: Is the kernel a subring of R?

Let's see. Given $a, b \in \ker\varphi$ we have

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

hence $a+b \in \ker\varphi$, and

$$\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0$$

hence $ab \in \ker\varphi$. Also we have $0_R \in \ker\varphi$ because

$$\varphi(0_R) = \varphi(0_R + 0_R)$$
$$= \varphi(0_R) + \varphi(0_R)$$

$$\Rightarrow \varphi(0_R) = 0_S.$$

But (WARNING) we probably have

$$1_R \notin \ker \varphi.$$

Indeed, suppose that $1_R \in \ker \varphi$. Then for any $a \in R$ we have

$$\varphi(a) = \varphi(a 1_R) = \varphi(a)\varphi(1_R)$$
$$= \varphi(a) \cdot 0 = 0.$$

So φ is the zero map!
(That's not interesting.)

So $\ker \varphi \subseteq R$ is not a subring (unless $\varphi = 0$). What is it?

Definition: Let R be a ring. A subset $I \subseteq R$ is called an ideal if

- I is a subgroup of $(R, +, 0)$
- $a \in R, x \in I \Rightarrow ax \in I$. ///

Equivalently, if we think of R as a module over itself via multiplication

$$\mu : R \to \mathrm{Aut}(R^+)$$
$$a \longmapsto (b \mapsto ab).$$

Then ideal $\equiv$ submodule of R.

Thus ideals are analogous to sub vector spaces. Given any elements $a_1, a_2, \ldots, a_k \in I$ we define the ideal <u>generated</u> by $a_1, \ldots, a_k$:

$$(a_1, \ldots, a_k) := \{ r_1 a_1 + \cdots + r_k a_k : r_i \in R \}$$

"linear combinations".

An ideal $I \subseteq R$ is <u>principal</u> if

$$I = (a) \quad \text{for some } a \in R \qquad //$$

If $\varphi : R \to S$ is a ring map, note that $\ker \varphi \subseteq R$ is an <u>ideal</u>. Indeed, for all $a \in R$, $x \in \ker \varphi$ we have

$$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0 = 0$$

$$\Longrightarrow \quad ax \in \ker \varphi.$$

Conversely, we have the following.

Theorem: Let R be a ring and let $I \subseteq R$ be a subset. Then

I is an ideal $\iff$ I is the kernel of a ring map $\varphi: R \to R'$.

Proof: We already showed $\Leftarrow$.

To show $\Rightarrow$ we must construct a ring R' and a map $\varphi: R \to R'$ from I.

Since I is a (normal) subgroup of the abelian group $(R, +, 0)$ we can form the quotient group

$$R/I = \{ a + I : a \in R \}$$

with well-defined operation

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

and identity element

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

We also have the natural surjective group homomorphism

$$\varphi : R \longrightarrow R/I$$
$$a \longmapsto a + I.$$

with $\ker \varphi = I$. Is φ also a ring map?

$$\varphi(ab) = (ab) + I \overset{?}{=} \text{“}\varphi(a)\varphi(b)\text{”}$$
$$= \text{“}(a+I)(b+I)\text{”}$$

Let's see if this works. Define

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

If $a + I = a' + I$ and $b + I = b' + I$ (i.e. $a = a' + x$ and $b = b' + y$ for some $x, y \in I$) then we have

$$ab = (a'+x)(b'+y)$$
$$= a'b' + (a'y + b'x + xy).$$

Since $ab - a'b' \in I$
we conclude that $(ab) + I = (a'b') + I$.

So it works. The quotient R/I is a ring and the canonical map

$$\varphi : R \to R/I$$
$$a \mapsto a + I$$

is a ring map with $\ker \varphi = I$. 

[Note: The concepts of ideal and quotient ring were forced on us by the concept of ring map. We had no choice.]

By analogy with groups, we can prove several isomorphism theorems.

Let $\varphi : R \to S$ be a ring map. Then we have a ring isomorphism

$$\bar{\varphi} : R/\ker\varphi \to \operatorname{im}\varphi$$
$$a + (\ker\varphi) \mapsto \varphi(a)$$

Proof omitted.

Let $\mathcal{L}(R) = \{\text{ideals } I \leq R\}$. This is a lattice with

$$\hat{0} = (0) = \{0\} \quad , \quad \hat{1} = (1) = R.$$
$$I \wedge J = I \cap J \quad , \quad I \vee J = I \cup J$$

Given an ideal $I \leq R$ we also have a lattice $\mathcal{L}(I, R) = \{\text{ideals } I \leq J \leq R\}$ with $\hat{0} = I$.

If $J \in \mathcal{L}(I, R)$ then the set

$$J/I := \{a + I : a \in J\} \subseteq R/I$$

is an ideal of R/I and.

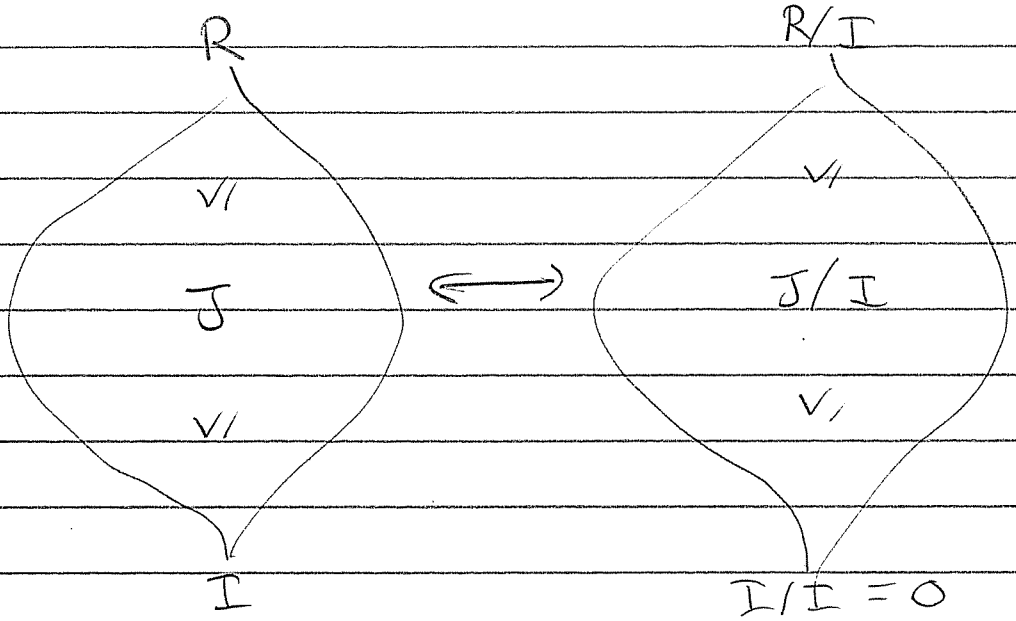
$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

If $S \subseteq R$ is a subring, $I \leq R$ an ideal, then

$$\frac{S+I}{I} \cong \frac{S}{S \cap I}$$

as rings

Finally, we have a lattice isomorphism



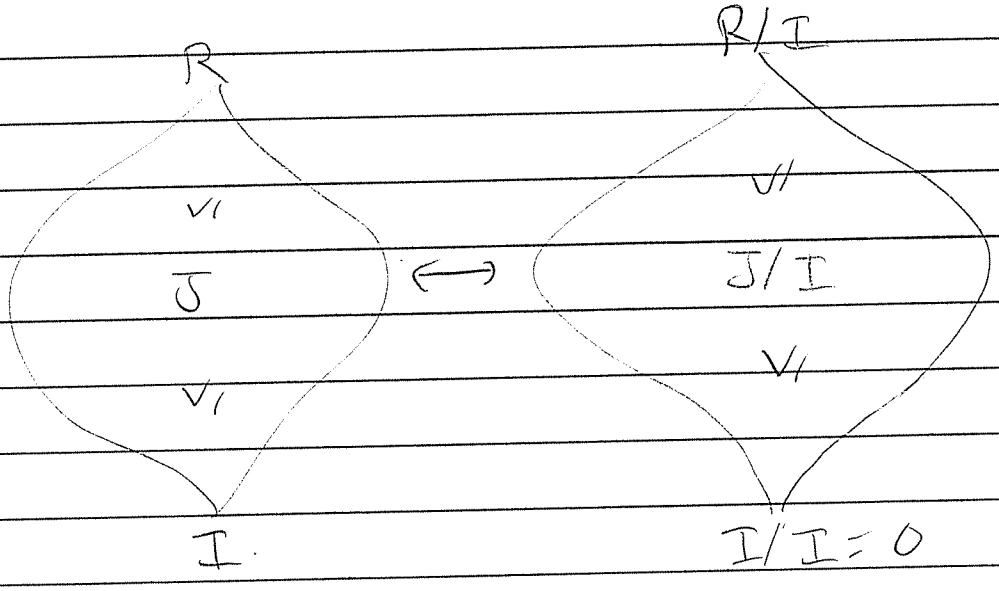
$$\mathcal{L}(I, R) \approx \mathcal{L}(R/I).$$

These things are too boring to prove. We will see geometric applications later.

1/28/14

HW 1 due next Tues Feb 4
(two typos fixed).
Office Hours: Mon 2-3, Wed 3-4.

Last time we discussed isomorphism theorems for rings, such as:



Today we will apply them.

Let R be a ring. We say that R is a field if

$$R^\times = R - \{0\}$$

Now we can give a new definition.

Theorem: R is a field if and only if R has only two ideals: (0) and $(1) = R$.

Proof: Suppose R is a field and consider a nonzero ideal $(0) \neq I \leq R$. There exists $0 \neq a \in I$ and since I is an ideal this implies $a^{-1}a = 1 \in I$. Hence for all $r \in R$ we have $r1 = r \in I$, i.e., $I = R$.

Conversely suppose R has no nontrivial ideal and consider $0 \neq a \in R$. Since $(a) \neq (0)$ we have $(a) = R$. Then since $1 \in R = (a)$, there exists $b \in R$ such that $1 = ab$. Hence R is a field. ///

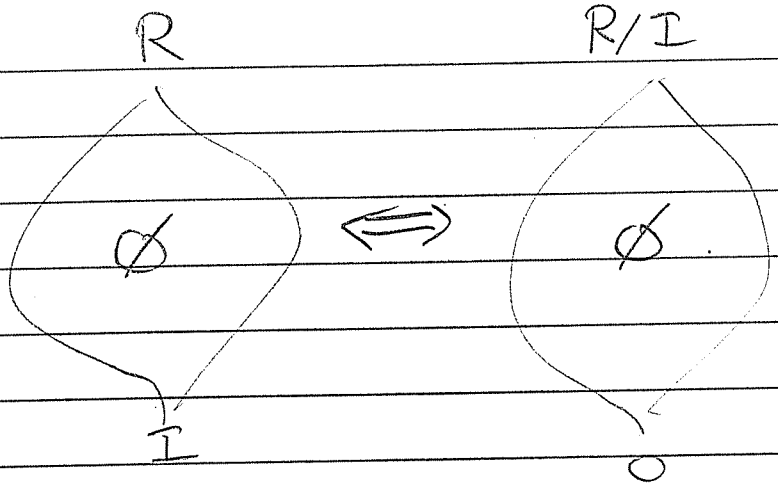
We say an ideal $m \leq R$ is **maximal** if

$$m \leq I \leq R \implies I = R.$$

Corollary: Let I be an ideal. We have

R/I is a field $\iff$ I is maximal.

Proof: We use the correspondence theorem:



The next simplest kinds of rings are the following.

Def: We say a ring R is <u>local</u> if it has a unique (nontrivial) maximal ideal $m \leq R$. In this case, R/m is the "residue field" of (R, m).

Examples:

(1) Let $p \in \mathbb{Z}$ be prime and consider the localization

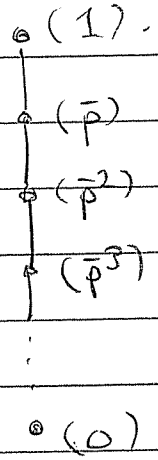
$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : a, b \in \mathbb{Z},\ p \nmid b \right\}$$

This ring is local with unique maximal ideal

$$(\bar{p}) = \{ p x : x \in \mathbb{Z}_{(p)} \}.$$

Proof: HW 1.4(a).

The only other ideals are $(\bar{p}^k)$ for $k \in \mathbb{N}$.
The lattice of ideals is a chain:



(residue field $\mathbb{Z}/p\mathbb{Z}$.)

(2) Let K be a field and consider the ring of formal power series

$$K[[x]] := \left\{ \sum_{i \geq 0}^{\infty} a_i x^i : a_i \in K \ \forall i \right\}.$$

with operations

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

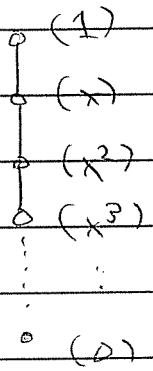
$$\left(\sum_i a_i x^i\right)\left(\sum_j b_j x^j\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k.$$

This ring is local with unique maximal ideal

$$(x) = \{ xf(x) : f(x) \in K[[x]] \}.$$

Proof: Maybe on HW 2.

Again, all ideals are of the form (x^k) and the lattice of ideals is a chain:



(residue field K)

Let R be a ring. We say R is a domain if

$$a, b \neq 0 \implies ab \neq 0 \quad \forall\, a, b \in R$$

Domains can also be characterized in terms of ideals.

Let $I \leq R$ be an ideal and suppose R/I is a domain. ↓

What does this tell us about I?

Suppose $a + I \neq I$ and $b + I \neq I$ (i.e. suppose $a \notin I$ and $b \notin I$). Then we must have

$$ab + I \neq I, \text{ hence } ab \notin I.$$

Def: Let $I \leq R$ be an ideal.
We say I is prime if

$$a, b \notin I \implies ab \notin I.$$
$$(ab \in I \implies a \in I \text{ or } b \in I).$$

This definition comes from Euclid's Lemma which says: given $a, b, p \in \mathbb{Z}$ with p prime we have

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$
$$(ab \in (p)) \quad (a \in (p) \text{ or } b \in (p)).$$

i.e. (p) is a prime ideal. ///

We have seen that R/I domain $\implies I$ prime.
The converse is also true.

Theorem: Let $I \leq R$ be an ideal. Then

R/I is a domain $\iff$ I is prime.

Proof: We already showed $\Rightarrow$. To show $\Leftarrow$ let $I \leq R$ be prime and suppose that $(a+I)(b+I) = (ab)+I = I$. Then $ab \in I$ and since I is prime this implies $a \in I$ or $b \in I$. In other words $a+I = I$ or $b+I = I$. Hence R/I is domain ///

Corollary: R is a domain if and only if the zero ideal (0) is prime. ///

Note that every maximal ideal is prime since

I max $\Rightarrow$ R/I field $\Rightarrow$ R/I domain $\Rightarrow$ I prime.

In fact, maximal ideals are sometimes called maximal primes.

In this class I want to give a geometric picture of maximal and prime ideals, and localizations of these.

First Example: Let

$$R = C^0[0,1] = \{\text{continuous } f : [0,1] \to \mathbb{R}\}$$

with pointwise addition and multiplication

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$

Given any subset $X \subseteq [0,1]$ consider the functions that vanish on X,

$$I(X) := \{f \in R : f(x) = 0 \ \forall x \in X\}$$

This is an ideal because given $f \in I(X)$ and $g \in R$ we have

$$fg(x) = f(x)g(x) = 0 \cdot g(x) = 0 \quad \forall x \in X,$$

hence $fg \in I(X)$.
When is this ideal maximal?

Theorem: Given any point $\alpha \in [0,1]$ the ideal $I_\alpha := I(\{\alpha\}) = \{f : f(\alpha) = 0\}$ is maximal.

Proof: Consider the evaluation function

$$ev_\alpha : R \longrightarrow \mathbb{R}$$
$$f(x) \longmapsto f(\alpha).$$

This is clearly a ring homomorphism. It is surjective because for all $\beta \in \mathbb{R}$ the constant function $[0,1] \to \mathbb{R}$ sending $x \mapsto \beta$ is continuous. Note that the kernel is I_α. Finally, since

$$R/I_\alpha \cong \mathbb{R}$$

is a field, we conclude that I_α is maximal. ///

This defines an injection

$$\text{points of } [0,1] \longrightarrow \text{max. ideals of } R$$
$$\alpha \longmapsto I_\alpha.$$

I claim this is a bijection.

Proof: We must show that every maximal ideal has the form I_α for some $\alpha \in [0,1]$. So let $m \subsetneq R$ be maximal and define the set

$$V(m) := \{ x \in [0,1] : f(x) = 0 \ \forall f \in m \}.$$

If $\exists\ \alpha \in V(m)$ then we have

$$I(V(m)) \subseteq I(\{\alpha\}) = I_\alpha.$$

Recall from the first lecture that we also have

$$m \subseteq I(V(m)) \subseteq I_\alpha.$$

Since m is maximal this implies $m = I_\alpha$.

So suppose $V(m) = \emptyset$, i.e., for all $x \in [0,1]$ there exists a function $f_x \in m$ with $f_x(x) \neq 0$. Let

$$U_x := \{ y \in [0,1] : f_x(y) \neq 0 \}$$

Then $\{ U_x : x \in [0,1] \}$ is an open cover of $[0,1]$. ↓

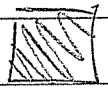
Since $[0,1]$ is compact, $\exists$ finite subcover

$$U_{x_1}, U_{x_2}, \dots, U_{x_k}.$$

The function $f_{x_1}^2 + f_{x_2}^2 + \cdots + f_{x_k}^2 \in m$ never vanishes, hence it is invertible

$$(f_{x_1}^2 + \cdots + f_{x_k}^2)^{-1} = \frac{1}{f_{x_1}^2 + \cdots + f_{x_k}^2}.$$

But this implies that $m = R$. Contradiction.



We obtain a bijection

points of $[0,1] \longleftrightarrow$ max. ideals of R.

Idea: Throw away $[0,1]$ and deal instead with the ring

$$R = C^\circ[0,1].$$

This is a very fruitful philosophy.

1/30/14

HW 1 due Tuesday.

Recall: Last time we saw a real world example.

Let X be a compact, Hausdorff space and consider the ring of continuous functions

$$R := C(X) = \{\text{continuous } f : X \to \mathbb{R}\}.$$

with pointwise $+$ & $\times$. For all subsets $A \subseteq X$ we define

$$I(A) := \{f \in C(X) : f(x) = 0 \ \forall\, x \in A\}$$

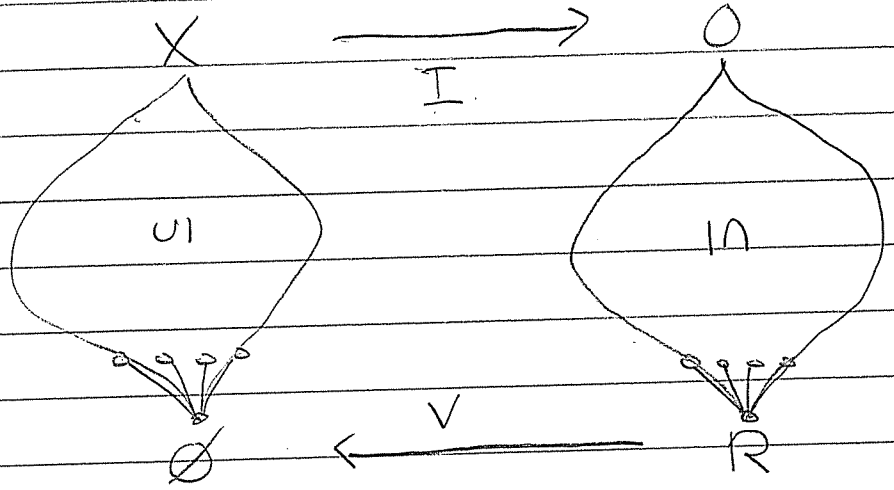
Note: This is an ideal $I(A) \trianglelefteq R$.
For all ideals $I \trianglelefteq R$ we define the vanishing locus

$$V(I) := \{x \in X : f(x) = 0 \ \forall\, f \in I\}.$$

Then by general nonsense (see 1st lecture) we have the following

- $\left.\begin{matrix} IV : 2^R \to 2^R \\ VI : 2^X \to 2^X \end{matrix}\right\}$ are closure operators

- We have an anti-isomorphism between lattices of closed sets:



This is called a "Galois connection".

Note that the minimal closed subsets of X are in bijection with the maximal closed ideals of R

Can we characterize these subsets/ideals?

Theorem: All points $\in X$ and all maximal ideals $\subseteq R$ are closed, so we get a bijection

$$\text{points } \alpha \in X \longleftrightarrow \text{max ideals } m \subseteq R$$
$$\alpha \longmapsto I(\alpha) := I(\{\alpha\})$$
$$V(m) \longmapsto m$$

Proof: We must show

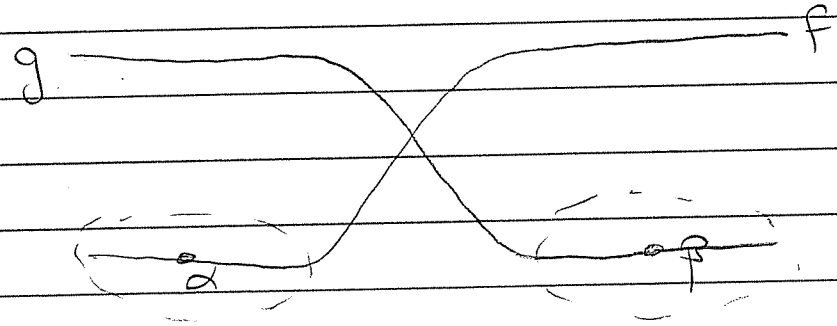
1. Every point has the form $V(m)$
2. Every max ideal has the form $I(\alpha)$.

1. Consider any point $\alpha \in X$. I claim That $\{\alpha\} = V(I(\alpha))$. Indeed, we have

$$\alpha \in V(I(\alpha))$$

Now suppose $\exists\, \beta \neq \alpha$ with $\beta \in V(I(\alpha))$. Since X is Hausdorff, the points α, β are closed. Then since X is compact, Urysohn's Lemma says $\exists$ continuous functions f, g such that

$$f(\alpha) = 0 \quad , \quad f(\beta) \neq 0$$
$$g(\alpha) \neq 0 \quad , \quad g(\beta) = 0$$



"points can be separated by functions"

But we assumed that $\beta \in V(I(\alpha))$, i.e, every function that vanishes at α also vanishes at β. The existence of f contradicts this. Hence

$$\{\alpha\} = V(I(\alpha))$$ ///

2. Consider any maximal ideal $m \leq R$. If $V(m) \neq \emptyset$ then choose $\alpha \in V(m)$. I claim that $m = I(V(m))$. Indeed, since $\{\alpha\} \subseteq V(m)$ we have

$$m \leq I(V(m)) \leq I(\alpha).$$

Then since m is maximal and $I(\alpha) \neq R$ [constants don't vanish at α] we have

$$m = I(V(m))$$

as desired. Otherwise, assume that $V(m) = \emptyset$, i.e., for all $\alpha \in X$ there exists $f_\alpha \in m$ with $f_\alpha(\alpha) \neq 0$.

↓

Define $U_\alpha := \{x \in X : f_\alpha(x) \neq 0\}$.

Then $\{U_\alpha : \alpha \in X\}$ is an open cover of X.
(open because $U_\alpha = f_\alpha^{-1}(\mathbb{R}-0)$ and $\mathbb{R}-0$ is open; cover because $\alpha \in U_\alpha$)
Since X is compact $\exists$ finite subcover

$$U_{\alpha_1}, U_{\alpha_2}, \dots, U_{\alpha_k}$$

Then the function $f_{\alpha_1}^2 + f_{\alpha_2}^2 + \cdots + f_{\alpha_k}^2 \in m$ never vanishes on X hence it's invertible.

$$(f_{\alpha_1}^2 + \cdots + f_{\alpha_k}^2)^{-1} = \frac{1}{f_{\alpha_1}^2 + \cdots + f_{\alpha_k}^2}.$$

But this implies $m = R$ (if $u \in m$ and u^{-1} exists then $u^{-1}u = 1 \in m \Rightarrow m = R$).
Contradiction.

We obtain a bijection

points of $X \longleftrightarrow$ max. ideals of $C(X)$.

[Remark: This is called the "weak Nullstellensatz" for R. It depends on the key property

$$V(I) = \emptyset \iff I = R.$$]

It turns out that $VI: 2^X \to 2^X$ is just the given topology on X.

Thus, if we can characterize the closure $IV: 2^R \to 2^R$ algebraically, we could replace X by R and lose no information.
[We would call this a "strong Nullstellensatz" for R.]

Unfortunately there is no nice answer in the ring $C(X)$. We get better results if we look at more "rigid" kinds of functions.

Topology $\not\longrightarrow$ Algebra

$C^0(X)$ continuous
$C^\infty(X)$ smooth
} "floppy"

$C^\omega(X)$ analytic ("GAGA")
$\mathbb{R}[x]$ polynomial
} "rigid"

If we work with "rigid" functions we will have a nice result:

Theorem (strong Nullstellensatz):

For all ideals $J \subseteq R$ we have

$$I(V(J)) = \sqrt{J} = \{f \in R : f^n \in J \text{ for some } n\}$$

The closed ideals $J = \sqrt{J}$ are called radical ideals.

In this case we can throw away the space X and work only with the ring.

Geometry ⟿ Algebra

:)

Again let X be compact Hausdorff and consider $R = C(X)$.

Q: What does localization of $C(X)$ mean?

Given point $\alpha \in X$ define the set

$$J(\alpha) := \{ f \in C(X) : f|_U = 0 \text{ for some open neighborhood } U \ni \alpha \}.$$

This an ideal since if $f|_U = 0$ then $(fg)|_U = 0$ for all $g \in C(X)$.

Definition: The quotient ring

$$C(X)/J(\alpha)$$

is called the ring of "germs" at α.

Given $f, g \in C(X)$ we get

$$f + J(\alpha) = g + J(\alpha)$$

$\iff$ $f = g$ on some open neighborhood of α.

Again let

$$I(\alpha) = \{ f \in C(X) : f(\alpha) = 0 \}.$$

Since $I(\alpha)$ is maximal (hence prime) we can define the localization at α:

$$C(X)_{I(\alpha)} := C(X)\left[(R - I(\alpha))^{-1}\right].$$

Theorem: We have

$$C(X)_{I(\alpha)} \cong C(X)/J(\alpha).$$

Proof sketch:

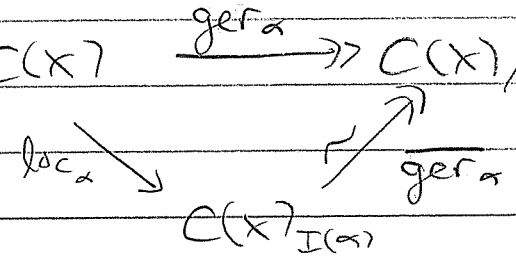
Consider the natural surjection

$$\begin{aligned} ger_\alpha : C(X) &\twoheadrightarrow C(X)/J(\alpha). \\ f &\longmapsto f + J(\alpha) \end{aligned}$$

Suppose $f \notin I(\alpha)$, i.e., $f(\alpha) \neq 0$.
Then $\exists$ nonvanishing g such that $f|_U = g|_U$ on some nbhd. of α.
Hence $f + J(\alpha)$ is invertible:

$$(f + J(\alpha))^{-1} = \left(\frac{1}{g} + J(\alpha)\right)$$

By the universal property of localization we have



We must show that $\overline{\mathrm{germ}}_a$ is injective. It's enough to show that loc_a sends any $f \in \mathcal{I}(a)$ to 0 in $C(X)_{\mathcal{I}(a)}$

So suppose $f \in \mathcal{I}(a)$, i.e, $f|_U = 0$ on some nbhd $U \ni a$. Then $\exists$ g with $g(a) = 1$ and $g = 0$ outside U (Urysohn), hence $fg \equiv 0$. Finally we have

$$\mathrm{loc}_a(f) = \frac{f}{1} = \frac{0}{g} = 0_{C(X)_{\mathcal{I}(a)}} \quad ///$$

This is the geometric meaning of localization.

One final remark about $C(X)$:
In the proof we found $f, g \in C(X)$ with

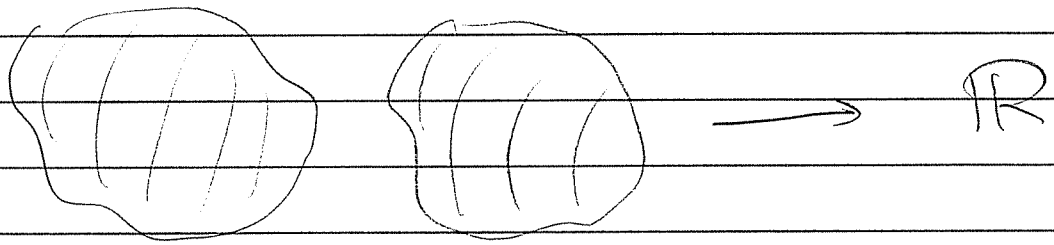
$$f, g \neq 0 \quad \text{but} \quad fg = 0$$

Hence $C(X)$ is not a domain ☹

For more "rigid" functions we will find that

R is a domain $\Longleftrightarrow$ X is "connected".

f: $\neq 0$ $\quad$ $= 0$
g: $= 0$ $\quad$ $\neq 0$



$$f, g \neq 0 \quad \text{but} \quad fg = 0.$$