Chapter 11
The prime spectrum

we're starting schemes!

<u>Main sources</u>: ① „Introduction to schemes" by Ellingsrud, Ottem
② „Geometry of schemes" Eisenbud, Harris

Before: affine varieties^{op} $\simeq$ reduced fin.gen. algebras over $k=\bar{k}$

Now: affine schemes^{op} $\simeq$ rings (assoc. comm. with 1)

This generalization allows to study arithmetic phenomena by geometric methods, by taking rings to be $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathcal{O}_K$ etc.

<u>Recall</u>: X affine k-variety, $k=\bar{k}$ => by Nullstellensatz points $x \in X \leftrightarrow$ max ideals $\mathfrak{m}_x \subset k[X]$
$\mathfrak{m}_x = \{f \in k[X] \mid f(x)=0\}$

<u>def.</u> R ring. Its <u>spectrum</u> is
$$\operatorname{Spec} R := \{\mathfrak{p} \mid \mathfrak{p} \subset R \text{ is a prime ideal}\}.$$

This way, $x \in \operatorname{Spec} R \leftrightarrow \mathfrak{p}_x \in R$ (motivation later!)

<u>NB</u>: in general, we cannot think about $f \in R$ as functions with values in a fixed field k.

However, there's a more general notion.

def. Let $x \in \operatorname{Spec} R$ correspond to $\mathfrak{p} \subset R$.
The residue field of x (or $\mathfrak{p}$) is

$$\kappa(x) = \kappa(\mathfrak{p}) := R_\mathfrak{p} / \mathfrak{p} \cdot R_\mathfrak{p}$$ — maximal ideal in $R_\mathfrak{p}$

unrelated to any particular k

Every element $f \in R$ has a „value"
$f(x) := f \bmod \mathfrak{p}_x \in \kappa(x)$ $\forall x \in \operatorname{Spec} R$,
and the codomain depends on the choice of x.

By definition, $f(x) = 0$ iff $f \in \mathfrak{p}_x$.

def.-Prop. The Zariski topology on $\operatorname{Spec} R$ is given by the closed subsets

$$Z(\mathfrak{a}) := \{x \in \operatorname{Spec} R \mid f(x) = 0 \ \forall f \in \mathfrak{a}\}$$
$$= \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq \mathfrak{a}\},$$
$\mathfrak{a} \subseteq R$ any ideal.

Prop. Let $\mathfrak{a}, \mathfrak{b} \subseteq R$ be ideals. Then
1) $Z(\mathfrak{a}) \subseteq Z(\mathfrak{b})$ iff $\sqrt{\mathfrak{a}} \supseteq \sqrt{\mathfrak{b}}$.
In particular, $Z(\mathfrak{a}) = Z(\sqrt{\mathfrak{a}})$.
2) $Z(\mathfrak{a}) = \emptyset$ iff $\mathfrak{a} = A$

3) $Z(\mathfrak{a}) = \operatorname{Spec} R$ iff $\mathfrak{a} \subseteq \sqrt{(0)} =: \operatorname{Nil} R$

nilradical

Proof uses the **Main Fact**: $\sqrt{\mathfrak{a}} = \bigcap\limits_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p}$.

In particular, $\mathfrak{p} \supseteq \mathfrak{a}$ iff $\mathfrak{p} \supseteq \sqrt{\mathfrak{a}}$, so

$Z(\mathfrak{a}) = Z(\sqrt{\mathfrak{a}})$.

1) $(\Rightarrow)$ $Z(\mathfrak{a}) \subseteq Z(\mathfrak{b}) \Rightarrow \underbrace{\bigcap\limits_{\mathfrak{p} \in Z(\mathfrak{a})} \mathfrak{p}}_{= \sqrt{\mathfrak{a}}} \supseteq \underbrace{\bigcap\limits_{\mathfrak{p} \in Z(\mathfrak{b})} \mathfrak{p}}_{= \sqrt{\mathfrak{b}}} \Rightarrow \sqrt{\mathfrak{a}} \supseteq \sqrt{\mathfrak{b}}$.

$(\Leftarrow)$ if $\mathfrak{p} \in Z(\mathfrak{a})$ and $\sqrt{\mathfrak{a}} \supseteq \sqrt{\mathfrak{b}}$, then $\mathfrak{p} \supseteq \sqrt{\mathfrak{a}} \supseteq \sqrt{\mathfrak{b}} \supseteq \mathfrak{b}$ implies $\mathfrak{p} \in Z(\mathfrak{b})$.

2) because $\sqrt{\mathfrak{a}} = (1)$ iff $\mathfrak{a} = (1)$, and $\mathfrak{p} \neq (1)$ $\forall \mathfrak{p}$, and $\forall \mathfrak{a} \subset \mathfrak{m}$ for some $\mathfrak{m}$.

3) because $Z(0) = \operatorname{Spec} R$.

Cor. There's an inclusion-reversing bijection

$$\left\{ \begin{array}{c} \text{closed subsets} \\ \text{of Spec } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{radical ideals} \\ \text{in } R \end{array} \right\}$$

$$Z(\mathfrak{a}) \longleftarrow\!\shortmid \ \mathfrak{a}$$

$$Z \longmapsto I(Z) := \bigcap_{\mathfrak{p} \in Z} \mathfrak{p} = \{ f \in R \mid f(x) = 0 \ \forall x \in Z \}$$

Cor. $\forall$ set $S \subseteq \operatorname{Spec} R$ its closure

$\overline{S} = Z(\mathfrak{a})$, where $\mathfrak{a} = \bigcap\limits_{\mathfrak{p} \in S} \mathfrak{p}$.

Proof: $\overline{S} = Z(\mathfrak{b})$, for some radical ideal $\mathfrak{b}$.

$\mathfrak{b} \subseteq \mathfrak{a}$: $\forall \mathfrak{p} \in S$ $\mathfrak{b} \subseteq \mathfrak{p}$.

$\mathfrak{b} \supseteq \mathfrak{a}$: $Z(\mathfrak{a}) \supseteq Z(\mathfrak{b})$ because $S \subseteq Z(\mathfrak{a})$ and $Z(\mathfrak{a})$ is closed, so $\overline{S} \subseteq Z(\mathfrak{a})$. ∎

In particular, for $S = \{p\}$ we get
$\overline{\{p\}} = Z(p) = \{q \in \operatorname{Spec} R \mid q \supseteq p \text{ prime}\}$.

Cor. $x \in \operatorname{Spec} R$ is a closed point iff p_x is a maximal ideal.

In Zariski topology, points don't have to be closed!
(unless R is of Krull dim 0)

Motivation: why prime ideals instead of maximal?
For varieties over $k = \bar{k}$, Nullstellensatz follows from the Jacobson property of f.g. reduced k-algebras, which tells that

$$\sqrt{I} = \bigcap_{m \supseteq I} m \quad \forall I \subset R,$$

and this property leads to the bijection between closed subsets and radical ideals.

In general, we must use prime ideals to get such a correspondence:
e.g. R a dvr $\Rightarrow \exists!\, m = (t) \subset R$,
but R has two radical ideals: (0) and (t),
so building Spec only out of max ideals wouldn't be enough.

§ Generic points

<u>def.</u> X top. space, $Z \subseteq X$ closed subset.
A generic point of Z (if exists) is a point $\eta \in Z$ s.t. $\overline{\{\eta\}} = Z$. a dense point!

In our context:
$\forall\, p$ is a generic point of $Z(p) \subseteq \operatorname{Spec} R$.

Main Ex.: R integral domain $\Rightarrow$
$p = (0)$ is the generic point of $\operatorname{Spec} R$,
because $\{q \supseteq (0) \mid q \text{ prime}\} = \operatorname{Spec} R$.

Rem. For general top. spaces, generic points can be non-unique, But for $X = \operatorname{Spec} R$ (and for schemes) we'll see that a generic point is unique $\forall\, Z \subseteq X$.

Ex. 1) $R = K$ a field
$\operatorname{Spec} K = \{(0)\}$ — single point

2) $R = K[t]/(t^n)$ thickening

$\operatorname{Spec} R = \{(t)\}$ — „thick" point
Note: (0) is not prime, because $t \cdot t^{n-1} \in (0)$
1) vs 2): same top. spaces, different algebraic structures

3) R Artinian ring

Spec R is a finite set;

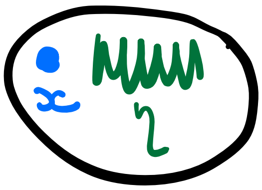
R local Artinian $\Rightarrow$ Spec R is a point

4) R dvr, e.g. $R = \mathbb{Z}_p$

Spec $R = \{x, \eta\}$ with $x \leftrightarrow \mathfrak{m}$ and $\eta \leftrightarrow (0)$.

Since x is a closed point,

the generic point $\eta = R - \{x\}$ is an open dense point!



Spec R

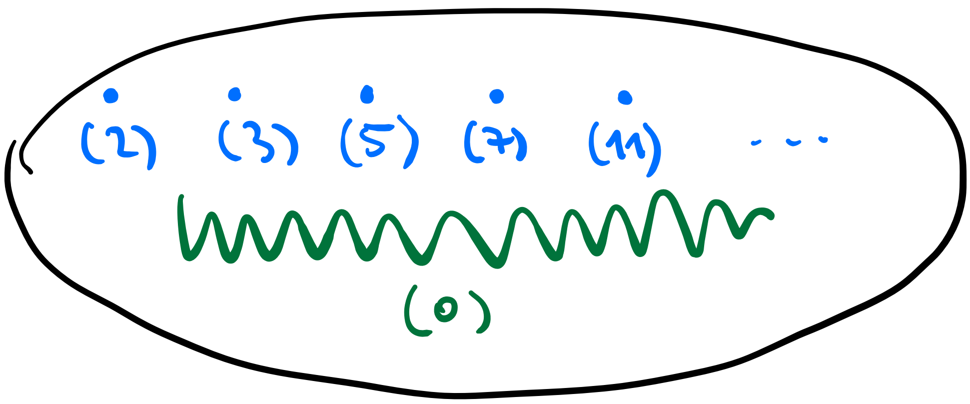
5) $R = \mathbb{Z}$

$$\mathrm{Spec}\, R \ni (0)$$
$$\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ni (p) \ \forall \text{ prime number } p$$

- $p\mathbb{Z} \subset \mathbb{Z}$ is maximal $\Rightarrow \{(p)\}$ is closed $\forall p$,
  and $\kappa(p) = \mathbb{Z}_p / p \cdot \mathbb{Z}_p = \mathbb{F}_p$
- $\mathbb{Z}(0) = \mathbb{Z} \Rightarrow \{(0)\}$ is the generic pt of Spec $\mathbb{Z}$,
  and $\kappa(0) = \mathbb{Z}_{(0)} = \mathbb{Q}$

So, every element $f \in \mathbb{Z}$ gives a „regular" function with values in various fields:

$$f = 17 \in \mathbb{Z} \rightsquigarrow \begin{aligned} f((0)) &= 17 \in \mathbb{Q} \\ f((2)) &= \bar{1} \in \mathbb{F}_2 \\ f((3)) &= \bar{2} \in \mathbb{F}_3 \\ f((5)) &= \bar{2} \in \mathbb{F}_5 \\ &\ldots \end{aligned}$$



Spec $\mathbb{Z}$

def. The affine n-space is

$$\mathbb{A}^n := \operatorname{Spec} \mathbb{Z}[t_1, .., t_n].$$

The affine n-space over R is

$$\mathbb{A}^n_R := \operatorname{Spec} R[t_1, .., t_n].$$

If $k = \bar{k}$, then

as a set

$$\mathbb{A}^n_k \supsetneq \mathbb{A}^n(k) = k^n$$

points are prime ideals in $k[t_1,..,t_n]$ — points are maximal ideals in $k[t_1,..,t_n]$,

and Zariski topology on $\mathbb{A}^n(k)$ is induced for Zariski topology on $\mathbb{A}^n_k$.

However, $\mathbb{A}^n_k$ has more points, e.g. (0).

Ex. ① $\mathbb{A}^1_{\mathbb{C}}$ – the affine line over $\mathbb{C}$
(or any $k=\bar{k}$)

- $(x-a) \leftrightarrow a \in \mathbb{C}$ closed pts
- $(0) = \eta$ generic pt

$$\kappa(a) = \mathbb{C}[x]_{(x-a)} / (x-a) \simeq \mathbb{C}$$

$$\kappa(\eta) = \mathbb{C}[x]_{(0)} = \mathbb{C}(x)$$

② $\mathbb{A}^1_{\mathbb{R}}$

$\mathbb{A}^1(\mathbb{R}) \ni$ • $(x-a)$, $a \in \mathbb{R}$ closed pts

$\mathbb{A}^1(\mathbb{R}) \not\ni$ • $(x-b)(x-\bar{b})$, $b \in \mathbb{C}$, $b \notin \mathbb{R}$ closed pts "of degree 2"

$\mathbb{A}^1(\mathbb{R}) \not\ni$ • $(0) = \eta$ generic pt

$$a \in \mathbb{R} \rightsquigarrow \kappa(a) \simeq \mathbb{R}$$

$$p = (x^2+1) \rightsquigarrow \kappa(p) \simeq \mathbb{R}[x] / x^2+1 \simeq \mathbb{C}\,!$$

real affine line has pts with complex residue fields

In general, $(f(t)) \in \mathbb{A}^1_k$ prime ideal $\Rightarrow$ $\kappa(f(t)) \supseteq k$ is the extension obtained by adjoining a root of f (irreducible polynomial).

§ Topology of Spec R

def. A distinguished open set in Spec R is
$D(f) := X - Z(f) = \{ p \in R \mid f \notin p \}$, $f \in R$.

Lemma. ① $D(f) = \emptyset$ iff $f \in R$ is nilpotent
② $D(f) \cap D(g) = D(fg)$
③ $D(g) \subseteq D(f)$ iff $g^n \in (f)$ for some $n \in \mathbb{N}$
④ $\{D(f)\}_{f \in R}$ is a basis of Zar topology on Spec R.
⑤ $\bigcup_{i \in I} D(f_i) = \operatorname{Spec} R$ iff
$\exists a_{i_1}, \dots, a_{i_N} \in R : \sum_{j=1}^{N} a_{i_j} f_{i_j} = 1$
In particular, Spec R is quasi-compact.

We can describe algebraically irreducibility of closed subsets in Spec R.

Prop. 1) $p \subset R$ prime $\Rightarrow \overline{\{p\}} = Z(p)$, and $\{p\}$ is the only generic point of $Z(p)$.

2) $Z \subseteq \operatorname{Spec} R$ closed subset is irreducible iff $Z = Z(p)$ for some p.

3) Spec R is irreducible iff the nilradical $\operatorname{Nil} R := \sqrt{(0)}$ is prime.

Cor. $\forall\, Z \overset{\neq \emptyset}{\subseteq} \operatorname{Spec} R$ irreducible closed subset has a unique generic point $\eta_Z \in Z$.

Rem. R integral domain $\Rightarrow$ Spec R irreducible but it's not a necessary condition:
$\operatorname{Spec} k[t]/(t^2) = \{(t)\}$ is a point, hence irreducible.

Proof of Prop.

1) $\overline{\{p\}} = Z(p)$ – ok,
uniqueness: $Z(p) = Z(q) \Rightarrow p \supseteq q$ and $q \subseteq p$.

2) $\Leftarrow$ $Z(p) = \overline{\{p\}}$ is irreducible because $\{p\}$ is.
$\Rightarrow$ let $Z(a) \subseteq \operatorname{Spec} R$ closed subset.
If $\sqrt{a} = \bigcap_{p \supseteq a} p$ is not prime, then
$\exists\, p \not\supseteq p' \supseteq a$, so we can write

$$\sqrt{a} = b \cap b', \text{ where } \sqrt{b} \neq \sqrt{b'}.$$

Hence $Z(a) = Z(b) \cup Z(b') \Rightarrow Z(a)$ not irreducible.

3) follows from 2) because $\operatorname{Spec} R = Z(\operatorname{Nil} R)$.

By the same argument as for varieties, we have:
Prop. R Noetherian, $Z \subseteq \operatorname{Spec} R$ closed subset $\Rightarrow$
$Z = Z_1 \cup \ldots \cup Z_r$, $Z_i \not\subseteq Z_j$, Z_i closed irreducible,
unique up to reordering. irreducible components

Exercise: $\operatorname{Spec}(R_1 \times R_2) \simeq \operatorname{Spec} R_1 \sqcup \operatorname{Spec} R_2$.

§ Morphisms between prime spectra

Another reason why we need prime ideals:
$\varphi: R \to S$ ring hom, $m \subset S$ max ideal $\Rightarrow$ $\varphi^{-1}(m) \subset R$ is not maximal in general, unlike for morphisms of varieties.

However, $\varphi^{-1}(m)$ is always prime, which will give us functoriality of Spec!

Ex: $k[x] \overset{i}{\hookrightarrow} k(x) \Rightarrow i^{-1}(0) = (0) \in k[x]$

closed pt   generic pt

Prop. There's a contravariant functor

$$\begin{aligned}
\mathrm{Spec}: \mathrm{Ring}^{op} &\to \mathrm{Top} \\
R &\longmapsto \mathrm{Spec}\, R \\
\varphi: R \to S &\longmapsto \varphi^*: \mathrm{Spec}\, S \to \mathrm{Spec}\, R \\
& \qquad\qquad \mathfrak{p} \longmapsto \varphi^{-1}\mathfrak{p}
\end{aligned}$$

Proof: $\mathfrak{p} \subset S$ prime $\Rightarrow \varphi^{-1}\mathfrak{p} \subset R$ also prime:
$a \cdot b \in \varphi^{-1}(\mathfrak{p}) \Rightarrow \varphi(ab) = \varphi(a)\cdot\varphi(b) \in \mathfrak{p} \Rightarrow \varphi(a)$ or $\varphi(b) \in \mathfrak{p}$.

Moreover, $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$ because $\psi^{-1}(\varphi^{-1}(\mathfrak{p})) = (\varphi\circ\psi)^{-1}(\mathfrak{p})$.
Clearly, $id^* = id$.
φ^* is continuous: see below

Lemma (Properties of φ^*, analogous to varieties)
Let $\varphi: R \to S$ ring hom, $\Phi := \varphi^*: \operatorname{Spec} S \to \operatorname{Spec} R$.

1) $\Phi^{-1}(Z(\mathfrak{a})) = Z(\varphi(\mathfrak{a}) \cdot S)$ $\forall$ ideal $\mathfrak{a} \subset R$.
In particular, Φ is continuous.

2) $\Phi^{-1}(D(f)) = D(\varphi(f))$ $\forall f \in R$

3) $\overline{\Phi(Z(\mathfrak{b}))} = Z(\varphi^{-1}(\mathfrak{b}))$ $\forall$ ideal $\mathfrak{b} \subset S$.

Prop. $\varphi: R \to S$ ring hom, $\Phi := \varphi^*: \operatorname{Spec} S \to \operatorname{Spec} R$.

1) If φ is surjective, then
$$\Phi: \operatorname{Spec} S \xrightarrow{\sim} Z(\operatorname{Ker} \varphi) \subseteq \operatorname{Spec} R$$
homeomorphism

2) If φ is injective, then
$\Phi(\operatorname{Spec} S) \subseteq \operatorname{Spec} R$ is dense.
Moreover, $\operatorname{Im} \Phi$ is dense iff $\operatorname{Ker} \varphi \subseteq \operatorname{Nil} R$.

Proof: 1) $\varphi: R \twoheadrightarrow S \Rightarrow S \simeq R/\mathfrak{a}$, $\mathfrak{a} = \operatorname{Ker} \varphi$.
$\{\mathfrak{p} \subset R/\mathfrak{a}\} \leftrightarrow \{\mathfrak{p} \subset R \mid \mathfrak{p} \supseteq \mathfrak{a}\}$, hence
Φ is a continuous bijection onto $Z(\operatorname{Ker} \varphi)$.
Φ is also closed: $\Phi(Z(\mathfrak{b}/\mathfrak{a})) = Z(\mathfrak{b})$.

2) by 3) of Lemma,
$\overline{\operatorname{Im} \Phi} = Z(\varphi^{-1}(0)) = Z(\operatorname{Ker} \varphi)$,
and $Z(\operatorname{Ker} \varphi) = \operatorname{Spec} R$ iff $\operatorname{Ker} \varphi \subseteq \operatorname{Nil} R$.

Ex. ① Quotients

$\mathfrak{a} \subset R$ ideal $\rightsquigarrow$
$$\begin{tikzcd} \operatorname{Spec} R/\mathfrak{a} \arrow[r] \arrow[dr, "\sim"'] & \operatorname{Spec} R \\ & Z(\mathfrak{a}) \arrow[u, phantom, "\cup"] \end{tikzcd}$$

it's a homeo onto a closed subset, i.e. a closed immersion.

② Localizations

$f \in R$ $\rightsquigarrow$
$$\begin{tikzcd} \operatorname{Spec} R_f \arrow[r] \arrow[dr, "\sim"'] & \operatorname{Spec} R \\ & D(f) \arrow[u, phantom, "\cup"] \end{tikzcd}$$

homeo onto an open subset — open immersion

③ Reductions

$\mathbb{Z} \twoheadrightarrow \mathbb{F}_p$ $\rightsquigarrow$
$$\begin{tikzcd} \operatorname{Spec} \mathbb{F}_p \arrow[r] \arrow[dr, "\sim"'] & \operatorname{Spec} \mathbb{Z} \\ & \{(p)\} \arrow[u, phantom, "\cup"] \end{tikzcd}$$

$\exists!\ \mathbb{Z} \to R$ $\rightsquigarrow$ $\operatorname{Spec} R \longrightarrow \operatorname{Spec} \mathbb{Z}$, and it factors through $\operatorname{Spec} \mathbb{F}_p$ iff R is of char p.

§ Fibers

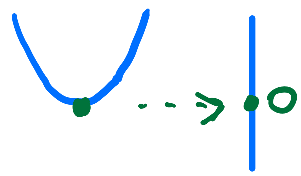
$\varphi : R \to S \rightsquigarrow \varphi^* : \operatorname{Spec} S \to \operatorname{Spec} R$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mathfrak{p} \in$

For $\mathfrak{p} \subset R$ we have: $(\varphi^*)^{-1}(\mathfrak{p}) = \{ \mathfrak{q} \subset S \mid \varphi^{-1}(\mathfrak{q}) = \mathfrak{p} \}$.

def. The **scheme-theoretic fiber** of φ^* over $\mathfrak{p}$ is $\operatorname{Spec} S \otimes_R \kappa(\mathfrak{p})$.

Points of this space are in bijection with $(\varphi^*)^{-1}(\mathfrak{p})$, because $S \otimes_R \kappa(\mathfrak{p}) \simeq S \otimes_R R_\mathfrak{p} / \mathfrak{p} \cdot R_\mathfrak{p} \simeq S_\mathfrak{p} / \mathfrak{p} \cdot S_\mathfrak{p}$.

Ex. $\mathbb{A}^1_k \to \mathbb{A}^1_k \qquad t \mapsto t^2$



Then the scheme-theoretic fiber over $0 = (t)$ is:

$$\operatorname{Spec} k[t] \underset{\substack{k[t] \\ t^2 \leftarrow\!\shortmid\, t}}{\otimes} k[t]/(t) = \operatorname{Spec} \underbrace{k[t]/(t^2)}_{\text{point of multiplicity } 2}$$

def. If R is a domain and $\eta = (0)$ (generic pt), we call fiber over η the **generic fiber**.

Moral: Generic fibers are useful for proving statements of type

„something good happens on a dense open subset":

$\varphi : X \xrightarrow{\text{good}} Y \rightsquigarrow \dim \varphi^{-1}(\eta_Y) = \dim X - \dim Y \implies$ (expect to happen) on a dense open $U \subseteq Y$ $\dim \varphi^{-1}(u) = \dim X - \dim Y$.

Ex. $\pi: \mathbb{A}^1_{\mathbb{C}} \to \mathbb{A}^1_{\mathbb{R}}$ canonical map

- $\pi^{-1}((0)) = (0)$
- $\pi^{-1}(t-a) = (t-a) \quad a \in \mathbb{R}$
- $\pi^{-1}((t-b)(t-\bar{b})) = \{(t-b), (t-\bar{b})\}, \qquad b \in \mathbb{C}, \; b \notin \mathbb{R}$

$\uparrow$ one point in $\mathbb{A}^1_{\mathbb{R}}$ $=$ $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-orbit of $(t-b)$

$\uparrow$ two points in $\mathbb{A}^1_{\mathbb{C}}$

This can be generalized as follows.

Thm. K field, L/K Galois extension, $G := \mathrm{Gal}(L/K)$.
Let A be a f.g. K-algebra, $A_L := A \otimes_K L$.
Then
$$\mathrm{Spec}\, A \simeq \mathrm{Spec}\, A_L/G$$
where $G \curvearrowright A_L$ via acting on L,
i.e. the points of $\mathrm{Spec}\, A$ correspond to G-orbits of points in $\mathrm{Spec}\, A_L$.

Main idea: G acts transitively on
$$\mathrm{Spec}\, E \otimes_K L \simeq \underbrace{\mathrm{Spec}\, E \otimes_A A_L}_{\text{any fiber}} \quad \forall\, E \supseteq K \text{ field extension.}$$

E.g.: $L/K = \mathbb{C}/\mathbb{R} \Rightarrow E \otimes_K L \cong E[t]/(t^2+1)$

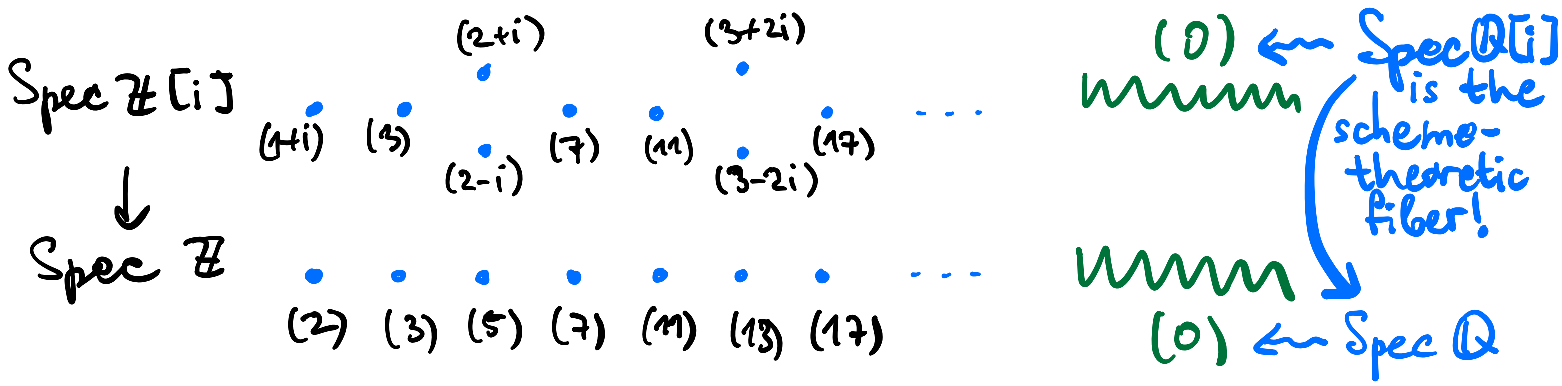
$\cong E(i)$ or $\cong E \times E$ two points

and $G: E \times E \xrightarrow{\text{swap}} E \times E$.

Ex. Gaussian integers

$$\varphi : \operatorname{Spec} \mathbb{Z}[i] \to \operatorname{Spec} \mathbb{Z}$$

Analyze $\operatorname{Spec} \mathbb{Z}[i]$ by looking at fibers of φ:
$p \equiv 3 \mod 4$ is prime in $\mathbb{Z}[i]$, whereas
$p \equiv 1 \mod 4$ decomposes as $(x+iy)(x-iy)$ in $\mathbb{Z}[i]$, hence:



In this case, $\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q})$ acts transitively on fibers.

Comments

- Points of Spec R have various residue fields, and this allows us to study simultaneously solutions of equations over different fields (or rings)

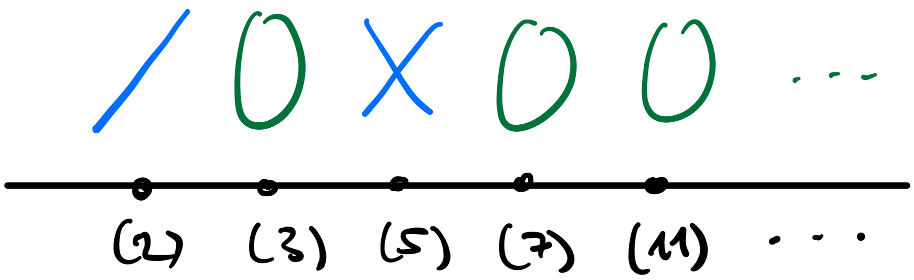
For example, fibers over $\operatorname{Spec} \mathbb{Z}$ could be given by solutions over $\mathbb{F}_p$'s and $\mathbb{Q}$

Ex: $\operatorname{Spec} \mathbb{Z}[x,y]/(x^2-y^2-5) \to \operatorname{Spec} \mathbb{Z}$

most fibers are usual conics, but some fibers are degenerate:

$x^2-y^2-5 \equiv (x+y+1)^2 \mod 2$;

$x^2-y^2-5 \equiv (x-y)(x+y) \mod 5$.



- When R is a f.g. k-algebra, $k=\bar{k}$, then $\forall$ closed point $\mathfrak{m}$ we have

$$\kappa(\mathfrak{m}) = k,$$

since by Weak Nullstellensatz $\kappa(\mathfrak{m}) \supseteq k$ is a finite field extension.

- For such R, the topology of $\operatorname{Spec} R$ is fully detected by the closed pts, that's why we didn't encounter the diversity of residue fields before — but having them lets us put number theory into geometric context and then some of us can prove results like Fermat's Last Thm! :)