Chapter 1

Hilbert's Nullstellensatz and applications

1.1 Fields of definition

When k is an algebraically closed field, Hilbert's Nullstellensatz gives us a bijection between algebraic subsets of k^n and radical ideals in $k[T_1, \ldots, T_n]$.

This correspondence induces an anti-equivalence of categories

$$\begin{aligned} \{\text{affine } k\text{-varieties}\} &\longleftrightarrow \{\text{finitely-generated reduced } k\text{-algebras}\} \\ (X, \mathcal{O}_X) &\longmapsto \mathcal{O}_X(X) \\ \hat{A} = \mathrm{Hom}_{k-\mathrm{alg}}(A, k) &\longleftarrow A. \end{aligned}$$

Lemma 1.1. *Let k be algebraically closed and A a finitely-generated k-Algebra. Then the map*

$$\begin{aligned} \hat{A} = \mathrm{Hom}_{k\text{-}alg}(A, k) &\longrightarrow \mathrm{Spm}\, A \\ \xi &\longmapsto ker\ \xi \end{aligned}$$

is a bijection.

Proof. The map admits an inverse

$$\begin{aligned} \mathrm{Spm}\, A &\longrightarrow \mathrm{Hom}_{k\text{-alg}}(A, k) \\ \mathfrak{m} &\longmapsto (A \to A/\mathfrak{m}). \end{aligned}$$

This is well-defined, since $A/\mathfrak{m}$ is a finite extension of the algebraically closed field k, so $k \simeq A/\mathfrak{m}$. □

Since we have defined a product on the left-hand side of the anti-equivalence, this must correspond to coproduct on the right-hand side. Since the coproduct in the category of commutative k-algebras with unit is given by the tensor product, we have

$$\mathcal{O}_{X \times Y}(X \times Y) \simeq \mathcal{O}_X(X) \otimes_k \mathcal{O}_Y(Y).$$

Corollary 1.2. *Let k be algebraically closed. Then the tensor product of two reduced (resp. integral) finitely-generated k-algebras is reduced (resp. integral).*

Proof. This follows from the anti-equivalence of categories: Reduced since products of affine k-varieties exist and integral since the product of two irreducible affine k-varieties is irreducible. □

Remark 1.3. 1.2 is false in general if $k = \overline{k}$. For instance $\mathbb{C}$ is an integral $\mathbb{R}$-algebra, but

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} &= \mathbb{R}[x]/(x^2+1) \otimes_{\mathbb{R}} \mathbb{C} \\ &= \mathbb{C}[x]/(x^2+1) \\ &= \mathbb{C}[x]/((x-i)(x+i)) \\ &\overset{(*)}{\simeq} \mathbb{C}[x]/(x-i) \times \mathbb{C}[x]/(x+i) \\ &\simeq \mathbb{C} \times \mathbb{C} \end{aligned}$$

is not integral, where $(*)$ follows from the Chinese remainder theorem.

For a non-reduced example, consider $k = \mathbb{F}_p(t)$ and choose a p-th root $\alpha = t^{\frac{1}{p}}$ in $\overline{\mathbb{F}_p(t)}$. Then $\alpha \notin k$ but $\alpha^n \in k$. If we put $L = k(\alpha)$, then $\alpha \otimes 1 - 1 \otimes \alpha \neq 0$ in $L \otimes_k L$ since the elements $(\alpha^i \otimes \alpha^j)_{0 \leq i,j \leq p-1}$ form a basis of $L \otimes_k L$ as a k-vector space, but

$$(\alpha \otimes 1 - 1 \otimes \alpha)^p = \alpha^p \otimes 1 - 1 \otimes \alpha^p = 1 \otimes \alpha^p - 1 \otimes \alpha^p = 0.$$

We now consider more generally finitely generated reduced k-algebras when k is not necessarily closed.

Example 1.4. Let $A = \mathbb{R}[X]/(x^2+1)$. Since x^2+1 is irreducible in $\mathbb{R}[x]$, it generates a maximal ideal, thus the finitely-generated $\mathbb{R}$-algebra A is a field and in particular reduced. We can equip the topogical space $X \coloneqq \operatorname{Spm} A = \{(0)\}$ with a sheaf of regular functions, defined by $\mathcal{O}_X(\{(0)\}) = A$. In other words, $\operatorname{Spm} A$ is just a point, but equipped with the reduced $\mathbb{R}$-algebra A. It thus differs from the point $\operatorname{Spm} \mathbb{R}$, which is equipped with the reduced $\mathbb{R}$-algebra $\mathbb{R}$, since $\mathbb{R}[x]/(x^2+1) \not\simeq \mathbb{R}$ as $\mathbb{R}$-algebras. Indeed, the $\mathbb{R}$-algebra $\mathbb{R}[x]/(x^2+1)$ is 2 dimensional as a real vector space.

A possesses a non-trivial $\mathbb{R}$-algebra automorphism induced by the automorphism of $\mathbb{R}$-algebras, $P \mapsto P(-x)$ in $\mathbb{R}[x]$. Indeed, $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ as $\mathbb{R}$-algebras, with the previous automorphism corresponding to the complex conjugation $z \mapsto \overline{z}$.

Example 1.5. By analogy with the Zariski topology on maximal spectra of (finitely generated, reduced) $\mathbb{C}$-algebras, we can equip $X = \operatorname{Spm} A$ with a Zariski topology for all (finitely generated reduced) $\mathbb{R}$-algebras A: the closed subsets of this topology are given by

$$\mathcal{V}_X(I) \coloneqq \{\mathfrak{m} \in \operatorname{Spm} A \mid \mathfrak{m} \supset I\}$$

for any ideal $I \subseteq A$. Note that $X = \operatorname{Spm} A$ contains $\hat{A} = \operatorname{Hom}_{k\text{-alg}}(A, k)$ as a subset: the points of $\hat{A}$ correspond to maximal ideals $\mathfrak{m}$ of A with residue field $A/\mathfrak{m} \simeq k$. But when $k \not\simeq \overline{k}$, the set $\operatorname{Spm} A$ is strictly larger than $\hat{A}$: it contains maximal ideals $\mathfrak{m}$ such that $A/\mathfrak{m}$ is a non-trivial finite extension of k. The induced topology on $\hat{A} \subseteq \operatorname{Spm} A$ is the Zariski topologoy of $\hat{A}$ that was introduced earlier.

Let $A = \mathbb{R}[x]$. Maximal ideals in the principal ring $\mathbb{R}[x]$ are generated by a single irreducible polynomial P, which is either of degree 1 or of degree 2 with negative discriminant.

In the first case, $P = x - a$ for some $a \in \mathbb{R}$ and the residue field is $\mathbb{R}[x]/(x-a) \simeq \mathbb{R}$, while, in the second case, $P = x^2 + bx + c$ for $b, c \in \mathbb{R}$ and $b^2 - 4c < 0$ and by choosing a root z_0 of P in $\mathbb{C}$, the map

$$\begin{aligned} \eta_{z_0} \colon \mathbb{R}[x]/(x^2+bx+c) &\longrightarrow \mathbb{C} \\ \overline{P} &\longmapsto P(z_0) \end{aligned}$$

is a field-homomorphism. In particular it is injective. Since $\mathbb{C}$ and $\mathbb{R}[x]/(x^2+bx+c)$ are both degree 2 extensions of $\mathbb{R}$, we have $\mathbb{R}[x]/(x^2+bx+c) \simeq \mathbb{C}$. Note that the other root of x^2+bx+c is $\overline{z_0}$ and that $\eta_{\overline{z_0}} = \sigma \circ \eta_{z_0}$ where σ is complex conjugation on $\mathbb{C}$. So we have to ways to identify $\mathbb{R}[x]/(x^2+bx+c)$ to $\mathbb{C}$ and they are related by the action of $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ on $\mathbb{C}$.

To sum up, the difference between the two possible types of maximal ideals $\mathfrak{m} \subseteq \mathbb{R}[x]$ is the residue field, which is either $\mathbb{R}$ or $\mathbb{C}$. When it is $\mathbb{R}$, we find exactly the points of

$$\begin{aligned}\widehat{\mathbb{R}[x]} &= \mathrm{Hom}_{\mathbb{R}\text{-alg}}(\mathbb{R}[x], \mathbb{R}) \\ &\simeq \{\mathfrak{m} \in \operatorname{Spm} \mathbb{R}[x] \mid \mathbb{R}[x]/\mathfrak{m} \simeq \mathbb{R}\} \\ &\simeq \{(x-a)\colon a \in \mathbb{R}\} \\ &\simeq \mathbb{R}.\end{aligned}$$

And when the residue field is $\mathbb{C}$, we have $\mathfrak{m} = (x^2 + bx + c)$ with $b, c \in \mathbb{R}$ such that $b^2 - 4c < 0$. If we choose z_0 to be the root of $x^2 + bx + c$ with $\mathrm{Im}(z_0) > 0$, we can identify the set of these maximal ideals with the subset

$$H \coloneqq \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}.$$

In other words, the following pictures emerges, where we identify $\operatorname{Spm} \mathbb{R}[x]$ with

$$\hat{H} \coloneqq \{z \in \mathbb{C} \mid \mathrm{Im}(z) \geq 0\}$$

via the map

$$\begin{aligned}\operatorname{Spm} \mathbb{R}[x] &\longrightarrow \hat{H} \\ \mathfrak{m} &\longmapsto \begin{cases} a \in \mathbb{R} & \mathfrak{m} = (x-a) \\ z_0 \in H & \mathfrak{m} = ((x-z_0)(x-\overline{z_0})) \text{ and } \mathrm{Im}(z_0) > 0 \end{cases}\end{aligned}$$

which is indeed bijective. We see that $\operatorname{Spm} \mathbb{R}[x]$ contains a lot more points that $\mathbb{R}$. One could go further and add the ideal (0): This would give the set

$$\mathbb{A}^1_{\mathbb{R}} = \operatorname{Spec} \mathbb{R}[x] = \operatorname{Spm} \mathbb{R}[x] \cup \{(0)\}.$$

Remark 1.6. If A is a k-algebra and $\overline{k}$ is an algebraic closure of k, the group $\mathrm{Aut}_k(\overline{k})$ acts on the $\overline{k}$-algebra $A_{\overline{k}} \coloneqq A \otimes_k \overline{k}$ via $\sigma(a \otimes \lambda) \coloneqq a \otimes \sigma(\lambda)$. Moreover, the map $a \mapsto a \otimes 1$ induces an injective morphism of k-algebras $A \hookrightarrow A \otimes_k \overline{k}$ since the tensor product over fields is left-exact. Its image is contained in the k-subalgebra $\mathrm{Fix}_{\mathrm{Aut}_k(\overline{k})} A_{\overline{k}} \subseteq A_{\overline{k}}$. When k is a perfect field, this inclusion is an equality.

Example 1.7. If $A = \mathbb{R}[x]$, then $A \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}[x]$. The group $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle \sigma \rangle$ with $\sigma\colon z \mapsto \overline{z}$, acts naturally on $\mathbb{C}[x]$. This is an action by $\mathbb{R}$-algebra automorphisms. Clearly, $\mathrm{Fix}_{\langle \sigma \rangle} \mathbb{C}[x] = \mathbb{R}[x]$. There is an induced action on $\operatorname{Spm} \mathbb{C}[x]$, defined by

$$\sigma(\mathfrak{m}) = \sigma((x-z)) \coloneqq (x - \sigma(z)) = (x - \overline{z}).$$

When we identify $\operatorname{Spm} \mathbb{C}[x]$ with $\mathbb{C}$ via $(x-z) \mapsto z$, this action is just $z \mapsto \overline{z}$. This „geometric action" induces an action of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on regular functions on $\mathbb{C}$: to $h \in \mathcal{O}_{\mathbb{C}}(U)$, there is associated a regular function $h \in \mathcal{O}_{\mathbb{C}}(\sigma(U))$, defined for all $x \in \sigma(U)$, by

$$\sigma(h)(z) \coloneqq \sigma \circ h \circ \sigma^{-1}(z) = \overline{h(\overline{z})}.$$

In particular, if $h = P \in \mathcal{O}_{\mathbb{C}}(\mathbb{C}) = \mathbb{C}[x]$, then $P \mapsto \sigma(P)$ coincides with the natural $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ action on $\mathbb{C}[x]$. We will see momentarily that this defines a sheaf of $\mathbb{R}$-algebras on $\operatorname{Spm} \mathbb{R}[x]$. To that end, let us first look more closely at the $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ action on $\operatorname{Spm} \mathbb{C}[x]$. Its fixed-point set is

$$\{\mathfrak{m} \in \operatorname{Spm} \mathbb{C}[x] \mid \mathfrak{m} = (x-a), a \in \mathbb{R}\} \simeq \mathbb{R} = \mathrm{Fix}_{z \mapsto \overline{z}}(\mathbb{C}).$$

Moreover, there is a map

$$\begin{aligned}\operatorname{Spm} \mathbb{C}[x] &\longrightarrow \operatorname{Spm} \mathbb{R}[x] \\ \mathfrak{m} &\longmapsto \mathfrak{m} \cap \mathbb{R}[x]\end{aligned}$$

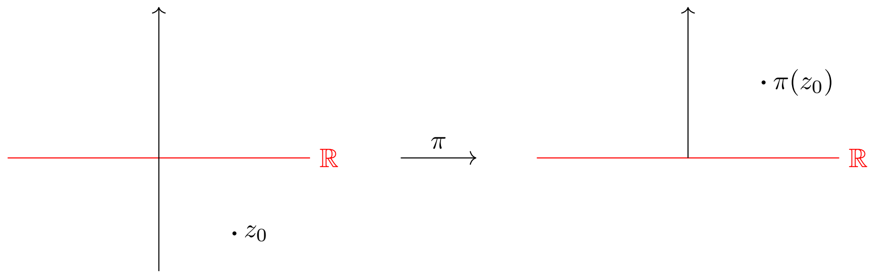

Figure 1.1: The quotient map $\pi\colon \operatorname{Spm}\mathbb{C}[x] \to \operatorname{Spm}\mathbb{R}[x]$ is geometrically a folding.

sending $(x-a)\mathbb{C}[x]$ to $(x-a)\mathbb{R}[x]$ if $a \in \mathbb{R}$, and $(x-z)\mathbb{C}[x]$ to $(x-z)(x-\overline{z})\mathbb{R}[x]$ if $z \in \mathbb{C} \setminus \mathbb{R}$. This map is surjective and induces a bijection

$$(\operatorname{Spm}\mathbb{C}[x])/\operatorname{Gal}(\mathbb{C}/\mathbb{R}) \xrightarrow{\simeq} \operatorname{Spm}\mathbb{R}[x].$$

Geometrically, the quotient map $\pi\colon \operatorname{Spm}\mathbb{C}[x] \to \operatorname{Spm}\mathbb{R}[x]$ is the „folding map“

$$\begin{aligned} \mathbb{C} &\longrightarrow \hat{H} \\ z = u + iv &\longmapsto u + i|v|. \end{aligned}$$

In view of this, it is natural to

(i) put the quotient topology on

$$\operatorname{Spm}\mathbb{R}[x] = (\operatorname{Spm}\mathbb{C}[x])\,/\operatorname{Gal}(\mathbb{C}/\mathbb{R})$$

where $\operatorname{Spm}\mathbb{C}[x] \simeq \mathbb{C}$ is equipped with its topology of algebraic variety.

(ii) define a sheaf of $\mathbb{R}$-algebras on $\operatorname{Spm}\mathbb{R}[x]$ by pushing-forward the structure sheaf on $\operatorname{Spm}\mathbb{C}[x]$ and then taking the $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-invariant subsheaf:

$$\mathcal{O}_{\operatorname{Spm}\mathbb{R}[x]}(U) \coloneqq \mathcal{O}_{\operatorname{Spm}\mathbb{C}[x]}(\pi^{-1}(U))^{\operatorname{Gal}(\mathbb{C}/\mathbb{R})}$$

where $\pi\colon \operatorname{Spm}\mathbb{C}[x] \to \operatorname{Spm}\mathbb{R}[x]$, $\mathfrak{m} \mapsto \mathfrak{m} \cap \mathbb{R}[x]$ is the quotient map, and $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ acts on $\mathcal{O}_{\operatorname{Spm}\mathbb{C}[x]}(\pi^{-1}(U))$ via $h \mapsto \sigma(h) = \sigma \circ h \circ \sigma^{-1}$ (note that the open set $\pi^{-1}(U)$ is $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-invariant).

Observe that

$$\mathcal{O}_{\operatorname{Spm}\mathbb{R}[x]}(\operatorname{Spm}\mathbb{R}[x]) = \mathbb{C}[x]^{\operatorname{Gal}(\mathbb{C}/\mathbb{R})} = \mathbb{R}[x].$$

Also, if $h = \frac{f}{g}$ around $x \in U$, then, around $\sigma(x) \in U$, one has $\sigma(h) = \frac{\sigma(f)}{\sigma(g)}$ and, for all $\lambda \in \mathbb{C}$, $\sigma(\lambda h) = \overline{\lambda}\sigma(h)$.

Remarkably, we will see that we can reconstruct the algebraic $\mathbb{C}$-variety

$$(X_{\mathbb{C}}, \mathcal{O}_{X_{\mathbb{C}}}) \coloneqq (\operatorname{Spm}\mathbb{C}[x], \mathcal{O}_{\operatorname{Spm}\mathbb{C}[x]})$$

from the ringed space

$$(X, \mathcal{O}_X) \coloneqq (\operatorname{Spm}\mathbb{R}[x], \mathcal{O}_{\operatorname{Spm}\mathbb{R}[x]}$$

that we have just constructed.