LECTURE 21, MONDAY MAY 10, 2004

FRANZ LEMMERMEYER

Let me start by recalling what we have done so far. Let $\mathcal{C}$ be a smooth projective curve in $\mathbb{P}^2K$, where K is some algebraically closed field. To every $f \in K(\mathcal{C})$ we have attached a divisor $\operatorname{div}(f) = \sum v_P(f)P$. For every divisor D we have defined a K-vector space

$$H^0(D) = \{f \in K(\mathcal{C}) : \operatorname{div}(f) + D \ge 0\}$$

whose dimension $h^0(D)$ is finite; the estimate

$$h^0(D) \ge \deg(D) + 1 - g$$

is called Riemann's Theorem and guarantees the existence of functions whose poles can only occur at certain places.

In fact, if $D = \sum n_i(P_i) - \sum m_j(Q_j)$, then $H^0(D)$ consists of all functions f with zeros of order $\ge m_j$ at Q_j and poles of order $\le n_i$ at P_i. Riemann's original motivation was to construct meromorphic functions on compact Riemann surfaces. For example, the meromorphic functions on a torus (which has genus 1) are exactly the elliptic functions. Riemann's Theorem says that $h^0(P) \ge 1$, which means that the meromorphic functions with at most a single pole at P have dimension at least 1: actually, the only such functions are constants. But Riemann's Theorem predicts $h^0(2P) \ge 2$, so there must exists nonconstant meromorphic functions whose only pole is at most a double pole at P: the only such functions are actually the Weierstrass $\wp$-functions.

In order to get a better understanding of what is going on, let us look at the simplest case of a function field: the field of rational functions with coefficients from $\mathbb{C}$, interpreted as the function field of the projective complex line. Note that the line has genus 0.

1. Rational Function Fields

Proposition 1.1. *For $f \in K(X)^\times$ we have $\deg \operatorname{div}(f) = 0$.*

Proof. Given a rational function $f = g/h \in K(X)^\times$, we can write it as a product of prime polynomials: we have $g = \alpha\prod(X - \alpha_i)^{a_i}$ for $\alpha_i \in K$ and $a_i \in \mathbb{Z}$, and $h = \beta\prod(X - \beta_j)^{b_j}$ for $\beta_j \in K$ and $b_j \in \mathbb{Z}$. Then $(f) = \sum a_iP_i - \sum b_jQ_j + (\deg h - \deg g)(P_\infty)$, where P_i and Q_j correspond to $X - \alpha_i$ and $X - \beta_j$. Thus $\deg \operatorname{div}(f) = \sum a_i - \sum b_j + \deg h - \deg g = 0$. □

Lemma 1.2. *If $\deg D < 0$, then $h^0(D) = 0$.*

In fact, if $D < 0$ then every $f \ne 0$ in $H^0(D)$ must have more zeros than poles. Thus $H^0(D) = \{0\}$.

Lemma 1.3. *If $\deg D = 0$, then $h^0(D) = 1$.*

Proof. Write $D = \sum n_i P_i - \sum m_j Q_j$; we know that $N = \sum n_i = \sum m_j$. The only monic polynomial with zero divisor $\sum n_i P_i$ is $g(X) = \prod (X - \alpha_i)^{n_i}$, where $X - \alpha_i$ corresponds to P_i; we have $\operatorname{div}(g) = \sum n_i P_i - N\infty$. Similarly, the only monic polynomial with pole divisor $\sum m_j Q_j$ is $1/h(X)$, where $h(X) = \prod (X-\beta_i)^{m_i}$ and where $X - \beta_j$ corresponds to Q_j; note that $\operatorname{div}(h) = \sum m_j Q_j - N\infty$. Thus $f = g/h$ has the right zeros and poles: $\operatorname{div}(f) = \operatorname{div}(g) - \operatorname{div}(h) = D$. Since we did not have any choices, f is the only solution up to scalar multiples, in other words: $H^0(D) = f \cdot K^\times \cup \{0\} = f \cdot K$. □

Since we are mainly interested in knowing that certain functions exist, the essential information in the last lemma is that $h^0(D) \ge 1$; since $g = 0$, this is exactly what Riemann's theorem tells us.

Lemma 1.4. *For $P \ne \infty$ we have $H^0(P) = f_1 \cdot K + f_2 \cdot K$, where $f_1 = \frac{1}{X-a}$ and $f_2 = \frac{X}{X-a}$, and where P corresponds to $X - a$.*

Proof. If $f \in H^0(P)$, then f may have a simple pole at P. Writing $f = g/h$, we find that $h = X - a$. Moreover, $\deg g \le \deg h$ since f is not allowed to have a pole at infinity, hence $g = rX + s$ for some constants $r, s \in K$. Thus $f = \frac{rX+s}{X-a} = r\frac{X}{X-a} + s\frac{1}{X-a}$. □

Lemma 1.5. *For $P \ne \infty$, the space $H^0(nP)$ has K-basis*

$$\Big\{\frac{1}{(X-a)^n}, \frac{X}{(X-a)^n}, \dots, \frac{X^n}{(X-a)^n}\Big\}.$$

Proof. If $f \in H^0(P)$, then f may have a pole of multiplicity $\le n$ at P. Writing $f = g/h$, we find that $h = (X-a)^n$ (allowing common factors of g and h). Moreover, $\deg g \le \deg h$ since f is not allowed to have a pole at infinity, hence $g = a_0 + a_1 X + \dots + a_n X^n$ for some constants $a_i \in K$. This proves the claim. □

Lemma 1.6. *The space $H^0(n\infty)$ has K-basis $\{1, X, \dots, X^n\}$.*

Proof. No $f \in H^0(n\infty)$ has a pole at some finite point, hence f is a polynomial. Since it has a pole of multiplicity $\le n$ at infinity, we have $\deg f \le n$. □

2. Schemes

In this last week of the semester I want to briefly explain the idea of schemes. It can be motivated by the analogy between local rings $\mathcal{O}_P(\mathcal{C})$ and the rings $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$. Here is what we know:

$\{$points on $\mathcal{C}\}$	$\{$prime ideals in $\mathbb{Z}\}$
$K[\mathcal{C}]$	$\mathbb{Z}$
$\mathcal{O}_P(\mathcal{C})$	$\mathbb{Z}_{(p)}$
$\mathfrak{m}_P$	(p)
$\mathcal{O}_P(\mathcal{C})/\mathfrak{m}_P \simeq K$	$\mathbb{Z}_{(p)}/(p) \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$
$K(\mathcal{C})$	$\mathbb{Q}$
$\cap_P \mathcal{O}_P(\mathcal{C}) = K[\mathcal{C}]$	$\cap_p \mathbb{Z}_{(p)} = \mathbb{Z}$

Classical algebraic geometry studies the objects on the left hand side. Krull had the idea of generalizing this theory to include onjects such as those on the right hand side, and this idea was rediscovered by Grothendieck who created the theory of schemes.

3. The Spectrum of Rings

Prime Ideals. Let R be a commutative ring with unit. The spectrum of R will be the set of prime ideals in R; before we introduce it, let us recall the definition and the basic properties of prime ideals. An ideal $\mathfrak{p} \neq R$ is called a prime ideal if $R/\mathfrak{p}$ is an integral domain (thus $\mathfrak{p} \neq R$ since we demand that integral domains have at least two elements, namely 0 and $1 \neq 0$), and a maximal ideal if $R/\mathfrak{p}$ is a field. Since fields are integral domains, maximal ideals are always prime. The converse is not necessarily true: consider $R = \mathbb{Z}[X]$ and $\mathfrak{p} = (2)$; then $R/\mathfrak{p} \simeq \mathbb{F}_2[X]$ is an integral domain, so $\mathfrak{p}$ is prime, but $R/\mathfrak{p}$ is not a field, and consequently $\mathfrak{p}$ is not maximal.

Now we define $\operatorname{Spec} R$ to be the set of prime ideals of R.

Examples.

- $\operatorname{Spec} 0 = \varnothing$ (note that 0 is a ring with identity $0 = 1$ by convention).
- $\operatorname{Spec} F = \{(0)\}$ for fields F.
- $\operatorname{Spec} \mathbb{Z} = \{(0), (2), (3), (5), (7), (11), \ldots\}$; note that the zero ideal (0) is prime since $\mathbb{Z}/(0) \simeq \mathbb{Z}$ is a domain. Clearly (0) is the only prime ideal in $\mathbb{Z}$ that is not maximal.
- $\operatorname{Spec} F[X] = \{(0)\} \cup \{(X - a) : a \in F\}$, where F is an algebraically closed field. Since $F[X]/(0) = F[X]$ and $F[X]/(X - a) \simeq F$ are integral domains, (0) and the $(X - a)$ are indeed prime ideals. Conversely, if $\mathfrak{p} \neq (0)$ is prime, it is generated by a polynomial $f \in F[X]$; if f were constant, we would have $1 \in \mathfrak{p} = (f)$ and $\mathfrak{p} = F[X]$, hence $\deg f \geq 1$. If $\deg f > 1$, we could factor f into two nonconstant polynomials, say as $f = gh$ (note that F is algebraically closed), and then $F[X]/(f)$ has zero divisors in view of $[g + (f)][h + (f)] = 0$, so (f) is not prime. Thus $\mathfrak{p} = (f)$ for some linear polynomial as claimed.

You might want to find the spectrum of rings like $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{R}[X]/(X^2)$, $\mathbb{C}[X]/(X^2)$, $\mathbb{C}[X, Y]/(XY)$, ...

4. The Zariski Topology

Next we endow $\operatorname{Spec} R$ with a topology. This means that we have to specify which subsets of $\operatorname{Spec} R$ we want to view as being open; alternatively, since complements of open sets are closed and vice versa, we could specify which sets we regard as being closed. We have to make sure, however, that these closed sets satisfy the following axioms:

- $\varnothing$ and $\operatorname{Spec} R$ are closed.
- The union of two (or any finite number of) closed sets is closed.
- The intersection of any family of closed sets is closed.

For any ideal $\mathfrak{a}$ in R we put $V(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec} R : \mathfrak{a} \subseteq \mathfrak{p}\}$. Thus in $\mathbb{Z}$ we have $V((2)) = \{(2)\} = V((4))$ and $V((6)) = \{(2), (3)\}$.

Fact 4.1. *If $\mathfrak{a} \subseteq \mathfrak{b}$, then $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$.*

Proof. Let $\mathfrak{p} \in V(\mathfrak{b})$; then $\mathfrak{b} \subseteq \mathfrak{p}$, thus $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{p}$, hence $\mathfrak{p} \in V(\mathfrak{a})$. □

The converse of this lemma is false, as the example $V((2)) = V((4))$ in $\mathbb{Z}$ shows.

Proposition 4.2. *Let R be a ring; then*

(1) *$V(R) = \varnothing$ and $V((0)) = \operatorname{Spec} R$.*

(2) *for any pair of ideals* $\mathfrak{a}, \mathfrak{b}$ *in* R *we have* $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b})$.
(3) *for any family of ideals* $\mathfrak{a}_i$ *(*$i \in I$*), we have* $\bigcap_{i\in I} V(\mathfrak{a}_i) = V(\sum_{i\in I} \mathfrak{a}_i)$.

Proof. Since R is not a prime ideal, there is no prime containing R, hence we have $V(R) = \varnothing$. Similarly, every ideal contains the zero ideal (0), hence $V((0)) = \operatorname{Spec} R$.

2). Since $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$, we have $V(\mathfrak{a}) \subseteq V(\mathfrak{a} \cup \mathfrak{b})$. Similarly, $V(\mathfrak{b}) \subseteq V(\mathfrak{a} \cup \mathfrak{b})$, and we deduce that $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$.

Conversely, assume that $\mathfrak{p} \in V(\mathfrak{a} \cap \mathfrak{b})$. If $\mathfrak{p} \in V(\mathfrak{a})$, then we are done, so assume that $\mathfrak{p} \notin V(\mathfrak{a})$, i.e., that $\mathfrak{a} \subsetneq \mathfrak{p}$. Then there is an $a \in \mathfrak{a} \setminus \mathfrak{p}$. For any $b \in \mathfrak{b}$, we have $ab \in \mathfrak{a} \cap \mathfrak{b}$: since $a \in \mathfrak{a}$ and $b \in R$, we have $ab \in \mathfrak{a}$, and since $a \in R$ and $b \in \mathfrak{b}$, we have $ab \in \mathfrak{b}$. Thus $ab \in \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, and since $\mathfrak{p}$ is prime, we must have $b \in \mathfrak{p}$. Thus $\mathfrak{b} \subseteq \mathfrak{p}$ and $\mathfrak{p} \in V(\mathfrak{b})$.

3). Assume that $\mathfrak{p} \in \bigcap_{i\in I} V(\mathfrak{a}_i)$; then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for all $i \in I$, hence $\mathfrak{p} \in V(\sum_{i\in I} \mathfrak{a}_i)$.

Conversely, assume that $\mathfrak{p} \in V(\sum_{i\in I} \mathfrak{a}_i)$. Then $\sum_{i\in I} \mathfrak{a}_i \subseteq \mathfrak{p}$, hence $\mathfrak{a}_i \subseteq \mathfrak{p}$ and therefore $\mathfrak{p} \in V(\mathfrak{a}_i)$ for every $i \in I$, so finally $\mathfrak{p} \in \bigcap_{i\in I} V(\mathfrak{a}_i)$. □

This result shows that we can define a topology on $\operatorname{Spec} R$ by calling sets of the form $V(\mathfrak{a})$ closed. This topology is called the Zariski topology.

Fact 4.3. *The closure of a point* $\mathfrak{p}$ *is* $V(\mathfrak{p})$*. In particular, a point* $\mathfrak{p} \in \operatorname{Spec} R$ *is closed (in the Zariski topology) if and only if* $\mathfrak{p}$ *is maximal.*

Proof. The closure of a point $\mathfrak{p}$ is the intersection of all closed sets containing $\mathfrak{p}$; now $\mathfrak{p} \in V(\mathfrak{a})$ if and only if $\mathfrak{a} \subseteq \mathfrak{p}$, hence $V(\mathfrak{p}) \subseteq V(\mathfrak{a})$. Thus every such closed set contains $V(\mathfrak{p})$, and since $V(\mathfrak{p})$ is closed, the first claim follows.

As for the second claim, $V(\mathfrak{p})$ contains all prime ideals containing $\mathfrak{p}$; thus $V(\mathfrak{p}) = \{\mathfrak{p}\}$ if and only if $\mathfrak{p}$ is maximal. □

A point $\mathfrak{p} \in \operatorname{Spec} R$ is called a generic point if the $V(\mathfrak{p}) = \operatorname{Spec} R$. If R is an integral domain, then (0) is a generic point.

Thus if R is an integral domain with at least one nonzero prime ideal, then $\operatorname{Spec} R$ is not Hausdorff since in a Hausdorff space points are closed, whereas (0) is a prime ideal in R that is not maximal. This means that the spaces $\operatorname{Spec} R$ are almost never Hausdorff with respect to the Zariski topology.

Let us mention the following

Proposition 4.4. *The topological space* $\operatorname{Spec} R$ *is quasi-compact.*

Recall that a topological space is quasi-compact if it has the property that any open covering contains a finite subcovering. It is called compact if, in addition, the space is Hausdorff.

5. Spec as a Functor

Let $f : R \longrightarrow S$ be a ring homomorphism (note that we demand that $f(1) = 1$). Then we have a map $\operatorname{Spec} f : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$ defined by $\mathfrak{q} \longmapsto \mathfrak{p} = f^{-1}(\mathfrak{q})$ for $\mathfrak{q} \in \operatorname{Spec} S$. We have to show that $\mathfrak{p} \in \operatorname{Spec} R$. Assume therefore that $ab \in \mathfrak{p}$; then $f(a)f(b) = f(ab) \in \mathfrak{q}$, hence $f(a) \in \mathfrak{q}$ or $f(b) \in \mathfrak{q}$ since $\mathfrak{q}$ is prime in S. But then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, so $\mathfrak{p}$ is prime in R.

Another (better?) way of seeing this is by observing that f induces a homomorphism $R \longrightarrow S/\mathfrak{q}$ with kernel $\mathfrak{p} = f^{-1}(\mathfrak{q})$, hence we get a monomorphism $R/\mathfrak{p} \simeq \operatorname{im} f \hookrightarrow S/\mathfrak{q}$, that is, $R/\mathfrak{p}$ is contained in the integral domain $S/\mathfrak{q}$: but this implies that $\mathfrak{p}$ is a prime ideal.

Fact 5.1. *If $f : R \longrightarrow S$ is a ring homomorphism, then* $\operatorname{Spec} f : \operatorname{Spec} S \longrightarrow \operatorname{Spec} R$ *is continuous.*

Proof. We have to show that the preimage of closed sets is closed. Let $V(\mathfrak{a}) \subseteq \operatorname{Spec} R$ be a closed set. Then

$$\begin{aligned} \mathfrak{p} \in (\operatorname{Spec} f)^{-1} V(\mathfrak{a}) &\iff (\operatorname{Spec} f)(\mathfrak{p}) \in V(\mathfrak{a}) \\ &\iff f^{-1}(\mathfrak{p}) \in V(\mathfrak{a}) \\ &\iff \mathfrak{a} \subseteq f^{-1}(\mathfrak{p}) \\ &\iff f(\mathfrak{a}) \subseteq \mathfrak{p} \\ &\iff \mathfrak{A} \subseteq \mathfrak{p} \\ &\iff \mathfrak{p} \in V(\mathfrak{A}), \end{aligned}$$

where $\mathfrak{A}$ is the ideal generated by $\mathfrak{a}$; thus hence $(\operatorname{Spec} f)^{-1}(V(\mathfrak{a})) = V(f(\mathfrak{a}))$, showing that the preimage of a closed set is closed. □

We could summarize this result by saying that Spec is a contravariant functor from the category of rings (and ring homomorphisms) to the category of topological spaces (and continuous maps).

The inclusion $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$ induces a map $\operatorname{Spec} \iota : \operatorname{Spec} \mathbb{Q} \longrightarrow \operatorname{Spec} \mathbb{Z}$; note that $\operatorname{Spec} \mathbb{Q} = \{(0)\}$, and that $\operatorname{Spec} \iota$ maps the zero ideal (0) in $\mathbb{Q}$ to the zero ideal in $\mathbb{Z}$. This example shows that $\operatorname{Spec} \iota$ does not induce a map between $\operatorname{Specm} \mathbb{Q}$ and $\operatorname{Specm} \mathbb{Z}$, since $\operatorname{Specm} \mathbb{Q} = \{0\}$ and $\operatorname{Specm} \mathbb{Z} = \{(2), (3), (5), (7), (11), \ldots\}$.

Note that if $f : R \longrightarrow S$ is an ring monomorphism (R is a subring of S), then $\mathfrak{p} = f^{-1}(\mathfrak{q})$ means $\mathfrak{p} = \mathfrak{q} \cap R$. Thus for the inclusion $\mathbb{Z} \longrightarrow \mathbb{Z}[i]$, the map $\operatorname{Spec} \mathbb{Z}[i] \longrightarrow \operatorname{Spec} \mathbb{Z}$ sends e.g. the prime ideal $(1 + 2i)$ in $\mathbb{Z}[i]$ to the prime ideal $(5) = (1 + 2i) \cap \mathbb{Z}$ in $\mathbb{Z}$.

Proposition 5.2. *If $f : R \longrightarrow S$ is a surjective ring homomorphism, then* $\operatorname{Spec} f$ *induces a homeomorphism ϕ between* $\operatorname{Spec} S$ *and the closed subset* $V(\ker f)$ *of* $\operatorname{Spec} R$.

Proof. We know that $\operatorname{Spec} f$ is continuous; if f is surjective, then the map ϕ induced by $\operatorname{Spec} f$ is bijective: first, given a prime ideal $\mathfrak{q} \in \operatorname{Spec} S$, the prime ideal $f^{-1}(\mathfrak{q})$ contains $\ker f$, hence is an element of $V(\ker f)$. Conversely, let $\mathfrak{p} \in \operatorname{Spec} R$ be a prime ideal containing $\ker f$; then $f(\mathfrak{p})$ is a prime ideal in S since f is surjective.

Since $\operatorname{Spec} f$ sends closed sets $V(\mathfrak{a})$ to closed sets $V(f^{-1}(\mathfrak{a}))$, it must be a homeomorphism. □

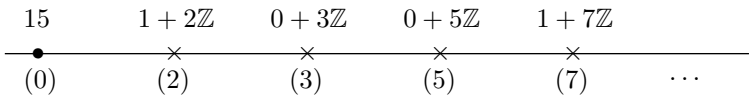
6. Elements as Functions

In the next chapter we shall introduce sheaves. Classically, these objects occur naturally as sheaves of functions on manifolds. It may therefore be helpful to become familiar with the idea that one may also consider the elements of a ring R as 'functions' on the 'manifold' $\operatorname{Spec} R$.

In fact, take an element $f \in R$ and a point $\mathfrak{p} \in \operatorname{Spec} R$; we have to define what $f(\mathfrak{p})$ should be. Observe that $R/\mathfrak{p}$ is an integral domain, so it has a quotient field $\kappa(\mathfrak{p})$. We now define $f(\mathfrak{p})$ to be the residue class $f + \mathfrak{p}$: thus elements $f \in R$ provide us with a 'function' $f : \operatorname{Spec} R \longrightarrow \kappa(\mathfrak{p})$. Observe that the target of f depends on the place $\mathfrak{p}$ where f is evaluated! Also observe that the addition of

ring elements f and g is compatible with the addition of f and g as functions since $(f+g)(\mathfrak{p}) = f(\mathfrak{p}) + g(\mathfrak{p})$.

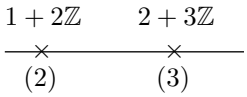
Example 1. If $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$, then $\mathbb{Z}/p = \mathbb{F}_p$ already is a field and $\kappa(\mathfrak{p}) = \mathbb{F}_p$. If $\mathfrak{p} = (0)$, then $\mathbb{Z}/(0) \simeq \mathbb{Z}$ and $\kappa(0) = \mathbb{Q}$ since $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$. Thus $15((7)) = 1 + 7\mathbb{Z}$: the element 15 maps the prime ideal (7) to the residue class $15 + 7\mathbb{Z} = 1 + 7\mathbb{Z}$. The graph of the function 15 would look something like this:



Example 2. Consider $R = \mathbb{C}[X]$; here $\operatorname{Spec} R$ consists of the prime ideal (0) and the maximal ideals $(X-a)$. We have $\kappa((0)) = \mathbb{C}(X)$, the field of rational functions with complex coefficients, and $\kappa((X-a)) = \mathbb{C}$ since $\mathbb{C}[X]/(X-a) \simeq \mathbb{C}$ via $f(x) \longmapsto f(a)$. Thus an element $f(X) \in \mathbb{C}[X]$ maps the maximal ideal $(X-a)$ to the residue class $f+(X-a)$, which we identify with $f(a) \in \mathbb{C}$ using the isomorphism above. Finally, $f \in \mathbb{C}[X]$ maps (0) to the coset $f + (0)$ in $\mathbb{C}(X)$.

As you can see, the value of functions at closed points gives you partial information, whereas the value at a generic point determines f. Let us now look at an example without a generic point:

Example 3. Now consider $R = \mathbb{Z}/6\mathbb{Z}$; we know that $\operatorname{Spec} R = \{(2), (3)\}$, and both ideals are maximal, hence all points are closed, and in particular there is no generic point. The function $f \in \mathbb{Z}/6\mathbb{Z}$ assumes the values $f \bmod 2$ and $f \bmod 3$ at the two points in $\operatorname{Spec} R$, and the Chinese Remainder Theorem guarantees that these two values determine f. As an exercise, determine the function f with the following two values:



$\operatorname{Spec} \mathbb{Z}/6\mathbb{Z}$

Proposition 6.1. *Let $f \in R$ and $\mathfrak{p} \in \operatorname{Spec} R$. Then $f(\mathfrak{p}) = 0$ if and only if $f \in \mathfrak{p}$.*

Proof. The image $f(\mathfrak{p})$ is the class $f + \mathfrak{p}$ in the quotient field of $R/\mathfrak{p}$; this element is 0 if and only if $f \in \mathfrak{p}$. □

Proposition 6.2. *Let $f \in R$ and $\mathfrak{p} \in \operatorname{Spec} R$. Then $f(\mathfrak{p}) \neq 0$ for all $\mathfrak{p} \in \operatorname{Spec} R$ if and only if $f \in R^\times$ is a unit.*

Proof. Assume that $f(\mathfrak{p}) \neq 0$ for all $\mathfrak{p} \in \operatorname{Spec} R$. If f is not a unit, then $(f) \neq R$, and there is a maximal ideal $\mathfrak{m} \supseteq (f)$. But then $f(\mathfrak{m}) = 0$: contradiction. Conversely, if f is a unit, then $fg = 1$ for some $g \in R$, and therefore $(f+\mathfrak{p})(g+\mathfrak{p}) = 1+\mathfrak{p}$; if we had $f(\mathfrak{p}) = 0$, then $(f+\mathfrak{p})(g+\mathfrak{p}) = 0+\mathfrak{p}$, and we would have $1 \in \mathfrak{p}$ contradicting the fact that $\mathfrak{p} \neq R$ for prime ideals $\mathfrak{p}$ by definition. □