Exercise Sheet 12

Exercise 1. Show that for a scheme X the following are equivalent:

a) X is reduced, i.e., for every open subset $U \subset X$ the ring $\mathcal{O}_X(U)$ has no non-zero nilpotent elements.

b) There is an open cover of X by affine schemes $U_i = \operatorname{Spec} R_i$ such that every ring $\mathcal{O}_X(U_i) = R_i$ has no non-zero nilpotent elements.

c) For every point $p \in X$, the local ring $\mathcal{O}_{X,p}$ has no non-zero nilpotent elements.

Solution.

a) a) $\implies$ b): Take any affine cover $\{U_i : i \in I\}$ of X, then by assumption all $\mathcal{O}_X(U_i)$ are reduced.

b) b) $\implies$ c): For $p \in X$ choose some element $U_i = \operatorname{Spec}(R_i)$ containing p (identifying $p \subseteq R_i$ as a prime ideal). Then $\mathcal{O}_{X,p} = (R_i)_p$ is a localization of R_i at p. This is reduced: assume that $a/b \in (R_i)_p$ was a nilpotent element, so that there exists $m \in \mathbb{N}$ such that $(a/b)^m = 0/1 \in (R_i)_p$. By definition this means that there is $s \in R_i \setminus p$ such that $s \cdot (a^m \cdot 1 - 0 \cdot b^m) = 0 \in R_i$. But this means $(s \cdot a)^m = s^{m-1} \cdot s \cdot a^m = 0 \in R_i$ which can only happen if $s \cdot a = 0 \in R_i$ as R_i is reduced. But then $s \cdot (a \cdot 1 - 0 \cdot b)$ shows that $a/b = 0/1 \in (R_i)_p$. Hence $(R_i)_p$ is reduced as desired.

c) c) $\implies$ a): Assume that $\varphi = (\varphi_p)_{p \in U} \in \mathcal{O}_X(U)$ is nilpotent, so that $0 = \varphi^m = (\varphi_p^m)_{p \in U}$. Then by definition $\varphi_p^m = 0 \in \mathcal{O}_{X,p}$ for all $p \in U$. Since all $\mathcal{O}_{X,p}$ are reduced, it follows $\varphi_p = 0$ for all $p \in U$ and thus $\varphi = 0$.

Exercise 2.

a) Let X be the scheme $\operatorname{Spec} \mathbb{Z}[x,y]/(x^2 + y^2 - 1)$ and $\mathbb{A}^1_{\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[t]$ be the affine line over $\mathbb{Z}$. Provide an explicit isomorphism

$$X \supseteq D(2(y-1)) \simeq D(2(t^2+1)) \subseteq \mathbb{A}^1_{\mathbb{Z}}$$

between open subschemes of X and $\mathbb{A}^1_{\mathbb{Z}}$.
Hint: It is useful to recall the proof of birational equivalence of an irreducible quadric and projective space over an algebraically closed field.

b) What are the $\mathbb{Q}$-points if X i.e. morphisms $\operatorname{Spec} \mathbb{Q} \to X$? Describe them explicitly using the isomorphism above. Use this to describe Pythagorean triples explicitly.

c) How many $\mathbb{F}_p$-points does X have? You can use the fact that the equation $t^2 = -1$ has a solution in $\mathbb{F}_p$ for odd p if and only if $p = 1 \mod 4$.

Solution.

a) By inspecting the birational equivalence between $V(x^2+y^2-z^2) =: X' \subset \mathbb{P}^2$ and $\mathbb{P}^1$ over an algebraically closed field of characteristic not 2 given by the projection from $(0:1:1) \in X'$ we see that in the affine coordinates it is given by $t \mapsto \frac{x}{1-y}$ and $x \mapsto \frac{2t}{1+t^2}; y \mapsto \frac{t^2-1}{t^2+1}$.

Denote $\mathcal{O}_X(X) = \mathbb{Z}[x,y]/(x^2+y^2-1)$ by R. The maps above can be used to define ring homomorphisms $\psi\colon R \to \mathbb{Z}[t][\frac{1}{t^2+1}]$ and $\phi\colon \mathbb{Z}[t] \to R[\frac{1}{y-1}]$. As we have $\psi(1-y) = 1 - \frac{t^2-1}{t^2+1} = \frac{2}{1+t^2}$ the first one extends to $R[\frac{1}{1-y}] \to \mathbb{Z}[t][\frac{1}{2(t^2+1)}]$ and hence to $\tilde{\psi}\colon R[\frac{1}{2(1-y)}] \to \mathbb{Z}[t][\frac{1}{2(t^2+1)}]$.

Similarly as $\phi(t^2+1) = (\frac{x}{1-y})^2 + 1 = \frac{x^2+1-2y+y^2}{(1-y)^2} = \frac{2(1-y)}{(1-y)^2} = \frac{2}{1-y}$ the second one extends to $\mathbb{Z}[t][\frac{1}{t^2+1}] \to R[\frac{1}{2(1-y)}]$ and hence to $\tilde{\phi}\colon \mathbb{Z}[t][\frac{1}{2(t^2+1)}] \to R[\frac{1}{2(1-y)}]$. Now we can see that $\tilde{\phi} \circ \tilde{\psi}$ and $\tilde{\psi} \circ \tilde{\phi}$ are identity maps hence giving an isomorphism $D(2(y-1)) \simeq D(2(t^2+1))$.

b) A morphism $f\colon \operatorname{Spec} \mathbb{Q} \to \operatorname{Spec} R$ is the same as a morphism $f^\#\colon R \to \mathbb{Q}$. Taking the images of x and y we see that these correspond to pairs $(x,y) \in \mathbb{Q}^2$ such that $x^2+y^2=1$. Using a) we see that if f factors through $D(2(y-1))$ then any such pair is given by $(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$ where $t \in \mathbb{Q}$. Otherwise we have $y=1$ so the pair is $(0,1)$.

Any nonzero triple $(a,b,c) \in \mathbb{Z}^3$ with $a^2+b^2=c^2$ gives rise to a $\mathbb{Q}$-point $(\frac{a}{c}, \frac{b}{c})$ on X and hence either $(a,b,c) = (0,k,k)$ or we have $(\frac{a}{c}, \frac{b}{c}) = (\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1})$ where $t \in \mathbb{Q}$. Writing $t = \frac{r}{s}$ with coprime integers r,s we see that the triple (a,b,c) is of the form $(2krs, k(r^2-s^2), \pm k(r^2+s^2))$.

c) If $p=2$ then the equation over $\mathbb{F}_2$ is equivalent to $x+y=1$ and there are exactly 2 solutions. Suppose p is odd.

Using the similar description but for $\mathbb{F}_p$-points we see that any $(x,y) \in \mathbb{F}_p^2$ with $x^2+y^2=1$ is either $(0,1)$ or arises from an $\mathbb{F}_p$-point of $D(2(t^2+1)) \subset \mathbb{A}^1_{\mathbb{Z}}$. Now we have $\mathbb{A}^1_{\mathbb{Z}}(\mathbb{F}_p) = D(2(t^2+1))(\mathbb{F}_p) \sqcup V(2(t^2+1))(\mathbb{F}_p)$ and $\mathbb{F}_p$-points of $V(2(t^2+1))$ correspond to solutions of $t^2+1=0$ in $\mathbb{F}_p$ so there are either 0 or 2 $\mathbb{F}_p$-points in $V(2(t^2+1))$. Putting all together we see that the number of solutions of $x^2+y^2=1$ over $\mathbb{F}_p$ for odd p is $p+1$ for $p = 3(\mod 4)$ and $p-1$ otherwise.

Exercise 3. Let X be a scheme and Z be a closed subset of the underlying topological space of X. Show that there is a unique closed subscheme Y of X such that its underlying topological space is Z and Y is reduced.

Solution. Suppose first that $X = \operatorname{Spec} R$ is an affine scheme and hence Z is the vanishing locus of an ideal $I \trianglelefteq R$. We see that $\operatorname{Spec}(R/\sqrt{I}) \hookrightarrow \operatorname{Spec} R$ is a reduced closed subscheme with the same underlying topological space. On the other hand for any closed subscheme $\operatorname{Spec}(R/J) \hookrightarrow \operatorname{Spec} R$ with the same underlying topological space we have $\sqrt{J} = \sqrt{I}$ so it defines J uniquely if it is reduced. Now if X is arbitrary we cover it with affines and use the uniqueness for any affine subscheme to deduce that the induced covering of Z endows it with a uniquely defined scheme structure. Reducedness follows from Exercise 1.

Exercise 4. Recall that for any $\mathbb{F}_p$-algebra R there is a morphism $x \mapsto x^p$ called the Frobenius morphism of R.

a) Let X be a scheme over $\mathbb{F}_p$ i.e. with a morphism $X \to \operatorname{Spec} \mathbb{F}_p$. Show that the structure sheaf takes values in $\mathbb{F}_p$-algebras and the Frobenius morphisms on affine charts glue uniquely to a morphism $\mathrm{Frob}\colon X \to X$ which is called the absolute Frobenius morphism of X.

b) Let X be a variety over $\mathbb{F}_p$. Describe the scheme–theoretic intersection of the graphs of Frob and identity in $X \times X$.

Solution.

a) For any open $U \subset X$ we have $U \to \operatorname{Spec} \mathbb{F}_p$ which is the same as giving a morphism $\mathbb{F}_p \to \mathcal{O}_X(U)$ so the structure sheaf takes values in $\mathbb{F}_p$-algebras. For any $\mathbb{F}_p$-algebra R the morphism Frob_R induces the identity morphism on the underlying topological space of $\operatorname{Spec} R$ so the Frobenius morphisms on the affine charts glue uniquely to the identity morphism on the underlying topological space of X.

The morphism of structure sheaves on any affine open $\operatorname{Spec} R$ then should be given by Frob_R which glue uniquely to the morphism $\mathrm{Frob}_{\mathcal{O}_X(U)}$ on any open U.

Note that Frob_X is functorial in X, i.e. for any morphism of schemes $f\colon X \to Y$ we have $f \circ \mathrm{Frob}_X = \mathrm{Frob}_Y \circ f$.

b) By the universal property of the fibre product we see that the scheme-theoretic intersection of Δ_X and Γ_{Frob_X} in $X \times X$ is given by a scheme Y with a morphism $f\colon Y \to X$ with the following property: for any morphism of schemes $g\colon Z \to X$ such that $\mathrm{Frob}_X \circ g = g$ there is a unique morphism $\phi\colon Z \to Y$ such that $g = f \circ \phi$. In particular $\mathrm{Frob}_X \circ f = f$ and by functoriality of Frobenius morphism we have $f \circ \mathrm{Frob}_Y = \mathrm{Frob}_X \circ f = f$. Which means that by the universal property described above we have $\mathrm{Frob}_Y = \mathrm{Id}_Y$. We claim that $Y \simeq \operatorname{Spec}(\mathbb{F}_p^{\oplus |X(\mathbb{F}_p)|})$.

Indeed, let us cover X by affine open subschemes $\operatorname{Spec} R_i$. Then the closed subscheme $\Delta_X \in X \times X$ is covered by $\operatorname{Spec} R_i \otimes R_i$ and $\Delta \cap \operatorname{Spec} R_i \otimes R_i$ is given by the ideal $(x \otimes 1 - 1 \otimes x)$ where $x \in R_i$. Similarly the subscheme $\Gamma_{\mathrm{Frob}_X} \cap \operatorname{Spec} R_i \otimes R_i$ is given by the ideal $(x \otimes 1 - (1 \otimes x)^p)$ where $x \in R_i$. So their intersection in $\operatorname{Spec} R_i \otimes R_i$ is isomorphic to $\operatorname{Spec}(R_i/(x^p - x))$, where $x \in R_i$. Hence these affine schemes cover Y and our claim then follows from the following claim:

Let R be a finitely generated $\mathbb{F}_p$-algebra. Then there is an isomorphism of rings $\tilde{R} := R/(x^p - x | x \in R) \simeq \mathbb{F}_p^{\oplus n}$, where $n \in \mathbb{N}$. Note that it follows automatically that n is the number of algebra homomorphisms from $\tilde{R}$ to $\mathbb{F}_p$ and since any homomorphism from R to $\mathbb{F}_p$ factors through $\tilde{R}$ this number is the same as the number of homomorphisms from R to $\mathbb{F}_p$.

Indeed, if $R \simeq \mathbb{F}_p[x_1, \cdots, x_m]$ then by Chinese remainder theorem or by induction on m we see that $\tilde{R} \simeq \mathbb{F}_p^{\oplus p^m}$. Now any finitely generated R is a quotient of a polynomial ring, hence $\tilde{R}$ is a quotient of $\mathbb{F}_p^{\oplus p^m}$ and hence is isomorphic to $\mathbb{F}_p^{\oplus n}$ for some n.