

LECTURE 36: MORE EXAMPLES

GIRJA SHANKER TRIPATHI

We continue our discussion of examples. In all these discussions we consider only algebraically closed fields. We'll denote any such field by k ; that is, $k = \bar{k}$, the closure of k .

Example 0.1. Let $S = \mathbb{A}_k^1 = \text{Spec } k[x]$. Consider $X = \text{Spec}(\frac{k[x,y]}{\langle y^2 - f(x) \rangle})$, where $f(x)$ is a square-free polynomial and $\text{char } k \neq 2$. (Just to recall: by square-free we mean that f has no roots of multiplicity more than 1.) Let $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$, with distinct α 's. Then X is affine subscheme of \mathbb{A}_k^2 . Consider the morphism $\pi : X \rightarrow S$ (this arises from the map $k[x] \rightarrow k[x, y]/\langle y^2 - f(x) \rangle$.)

We ask ourselves what are primes in the ring $\frac{k[x,y]}{\langle y^2 - f(x) \rangle}$:

Proposition 0.2. $\text{Spec}(k[x, y]/\langle y^2 - f(x) \rangle) = \{\{0\}, \langle \bar{x} - \alpha, \bar{y} \pm \sqrt{f(\alpha)} \rangle : \alpha \in k\}$.

Remark 0.3. Recall that an ideal $\bar{P} \subset k[x, y]/\langle y^2 - f(x) \rangle$ if and only if $P \subset k[x, y]$ is prime such that $\langle y^2 - f(x) \rangle \subset P$.

Proof. We first verify that all the ideals listed in the statement of the proposition are really prime ideals of the ring $k[x, y]/\langle y^2 - f(x) \rangle$. We know that $\{0\}$ is a prime ideal of a ring if and only if the ring itself is an integral domain. But, the ring $k[x, y]/\langle y^2 - f(x) \rangle$ is integral domain, if and only if $y^2 - f(x)$ is irreducible in $k[x, y]$. This is clearly true, since $f(x)$ is square-free. The ideals of $k[x, y]/\langle y^2 - f(x) \rangle$ of the form $\langle \bar{x} - \alpha, \bar{y} \pm \sqrt{f(\alpha)} \rangle$ are maximal, and hence prime.

Now we prove that a non-zero prime ideal of $k[x, y]/\langle y^2 - f(x) \rangle$ is of the form $\langle \bar{x} - \alpha, \bar{y} \pm \sqrt{f(\alpha)} \rangle$. Let $\bar{\mathcal{A}}$ be a prime ideal of $k[x, y]/\langle y^2 - f(x) \rangle$, and \mathcal{A} be the corresponding ideal of $k[x, y]$. Take a maximal ideal $\langle x - \alpha, y - \beta \rangle$ of $k[x, y]$ containing \mathcal{A} . Then by the above remark, we have $\langle y^2 - f(x) \rangle \subset \mathcal{A} \subset \langle x - \alpha, y - \beta \rangle$. Next, observe that $\langle g(x, y) \rangle \subset \langle x - \alpha, y - \beta \rangle$ if and only if $g(\alpha, \beta) = 0$. Therefore, $\beta = \pm \sqrt{f(\alpha)}$. This gives us $\mathcal{A} = \langle x - \alpha, y \pm \sqrt{f(\alpha)} \rangle$, and hence $\bar{\mathcal{A}} = \langle \bar{x} - \alpha, \bar{y} \pm \sqrt{f(\alpha)} \rangle$. □

Example 0.4. Let $S = \text{Spec}(\mathbb{Z})$, and let $K \subset \mathbb{Q}$ be a finite field extension of \mathbb{Q} . Consider $O_K \subset K$, the ring of integers of K ; that is, integral closure of \mathbb{Z} in K . Then we have a morphism $\bar{\pi} : \text{Spec}(O_K) \rightarrow \text{Spec}(\mathbb{Z})$, induced by the inclusion $\mathbb{Z} \hookrightarrow O_K$. For example, taking $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$,

we get $O_K = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ as ring of integers. We know that $\mathbb{Z}[i]$ is a unique factorization domain (although, in general, not all the rings of integers are unique factorization domains). In this case, we have $\text{Spec}(\mathbb{Z}[i]) = \{< 0 >, \text{ and maximal ideals } \}$. But in the ring $\mathbb{Z}[i]$, maximal ideals are of the following forms:

- (1) $< 1 + i > = < 1 - i > = \mathcal{A}$ (say). Observe that $2\mathbb{Z}[i] = \mathcal{A}^2$, since $2 = -i(1 + i)(1 - i)$ and $-i$ is unit in $\mathbb{Z}[i]$. We say that 2 ramifies over $K = \mathbb{Q}(\sqrt{-1})$;
- (2) $p\mathbb{Z}[i]$, where $p \equiv 3 \pmod{4}$. In this case, we say that p is inert or p remains prime; and
- (3) $p\mathbb{Z}[i]$, where $p \equiv 1 \pmod{4}$. In this case, we have $p = pp', p \neq p'$ (see below: the statement of a Fermat's Theorem and the following remark.) We say that the prime p splits.

Theorem 0.5. (Fermat's Theorem) *An odd prime p can be written as a sum of 2 squares of integers, if and only if, $p \equiv 1 \pmod{4}$.*

Remark 0.6. In view of Fermat's theorem stated above, for an odd prime $p \equiv 1 \pmod{4}$, we have $p = a^2 + b^2 = (a + bi)(a - bi) = pp'$. This provides a justification for the term that the prime p splits.

LOUISIANA STATE UNIVERSITY, DEPARTMENT OF MATHEMATICS, BATON ROUGE, LA 70803, USA

E-mail address: girja@math.lsu.edu