Math 510B Notes

Peter Kagey

Wednesday, January 16, 2019

Examples.

1. Let p be prime in $\mathbb{Z}$, then $x^n - p \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$.
2. Let $f(x,y) = y^4 - xy^3 - x^2y^2 + x \in \mathbb{Z}[x]$. Then write $\mathbb{Q}[x,y] = D[y]$ where $D = \mathbb{Q}[x]$. Since x is prime in D, $f(x,y)$ is irreducible in $\mathbb{Q}[x,y]$
3. Let $f(x,y)$ be irreducible in $\mathbb{Q}[x,y]$, then $g(x,y,z) = z^k + f(x,y)$ is irreducible in $\mathbb{Q}[x,y,z]$.
4. Let $f(x,y) = x^2 + y^2 - 1 \in \mathbb{R}[x,y] \cong R[x][y]$. This can be factored as $y^2 + (x+1)(x-1)$. Then using $x+1$ (or $x-1$) as the prime, $f(x,y)$ is prime by Eisenstein.
5. Let $f(x,y,z) = z^3 + x^2 + y^2 + 1$. Then let $p = x^2 + y^2 - 1 \in \mathbb{R}[x,y]$, so $z^3 + p$ is irreducible.
6. Let $g(x,y,z) = x^2z^3 - y^2z + xyz - x^2y$. Looking at this as a polynomial in z, this factors as $g(x,y,z) = x^2z^3 + (xy - y^2)z - x^2y$, so this is irreducible with prime y.

Example. Let D be a UFD and $p \in D$ a prime, then $D/\langle p \rangle$ might not be a UFD. For example, let $D = \mathbb{Z}[x]$ and $p = x^2 - 10$ which is irreducible in D, and thus prime.

$$\frac{D}{\langle p \rangle} \cong \frac{\mathbb{Z}[x]}{\langle x^2 - 10 \rangle} \cong \mathbb{Z}(\sqrt{10})$$

which is not a UFD; for example, $9 = 3^2 = (\sqrt{10}+1)(\sqrt{10}-1)$.

Lemma. Assume k is an algebraically closed field (e.g. $\mathbb{C}$). The maximal ideals of $k[x]$ are principal, generated by $(x-a)$ for some $a \in k$. In particular, the ideal $M_a := \langle x - a \rangle$ is the kernel of the specialization map $s_a \colon k[x] \to k$ which sends $f(x) \mapsto f(a)$ and thus $M_a \mapsto \langle 0 \rangle$. Thus there exists a $1-1$ correspondence between maximal ideals of $k[x]$ and the set k.

Proof. The ring $R = k[x]$ is a PID so $M = \langle p(x) \rangle$ for some $p(x)$ and M is maximal so M is a prime ideal, thus $p(x)$ is irreducible in R. Since k is closed, $p(x) = x - a$ for some $a \in k$ so $M = \langle x - a \rangle$. $\square$

Theorem. (Hilbert's Nullstellensatz over $\mathbb{C}$, weak form)
The maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ are of the form $M_{\overline{a}} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $\overline{a} = (a_1, \ldots, a_n)$. Thus, there exists a 1-1 correspondence between maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$ and $\overline{a} \in \mathbb{C}^n$, where $M_{\overline{a}}$ is the kernel of the map $f(x_1, \cdots, x_n) \mapsto f(a_1, \cdots, a_n)$.

Sublemma. Any polynomial f can be written as

$$f(\widetilde{x}) = f(\overline{a}) + \sum_i c_i(x_i - a_i) + \sum_{i,j} c_{ij}(x_i - a_i)(x_j - a_j) + \ldots$$

where the expression is finite because f is a polynomial.

Example. In $\mathbb{C}[x,y]$, let $\overline{a} = (1,-2)$ and $f(x,y) = x^2 + xy + 2$. Then let $x = u + 1$ and $y = v - 2$, so that

$$\begin{aligned} f(x,y) &= (u+1)^2 + (u+1)(v-2) + 2 \\ &= 1 + v + u^2 + uv \\ &= 1 + (y+2) + (x-1)^2 + (x-1)(y+2) \end{aligned}$$

Proof. The proof will proceed in two steps:

(1) The kernel $\ker(s_{\bar{a}}) = M_{\bar{a}}$, and this ideal is maximal in $\mathbb{C}[\widetilde{x}]$.

(2) Every maximal ideal of $\mathbb{C}[\widetilde{x}]$ is of the form $M_{\bar{a}}$ for some $\bar{a} \in \mathbb{C}^n$.

Proof of (1). Notice that $s_{\bar{a}} \colon \mathbb{C}[\widetilde{x}] \to \mathbb{C}$ is a surjective ring homomorphism, and so $\mathbb{C}[\widetilde{x}]/\ker(s_{\bar{a}}) \cong \mathbb{C}$ by the first isomorphism theorem for rings. Since the quotient is a field, $\ker(s_{\bar{a}})$ is maximal. Also, $M_{\bar{a}} \subset \ker(s_{\bar{a}})$ because each generator $s_{\bar{a}}(x_i - a_i) = 0$.
(...)

Proof of (2). Let M be maximal ideal so that $k = \mathbb{C}[\widetilde{x}]/M$ is a field, let $\pi \colon \mathbb{C}[\widetilde{x}] \to K$ be the usual quotient $x_i \mapsto \overline{x}_i$, and let $\pi_i = \pi|_{\mathbb{C}[x_i]} \colon \mathbb{C}[x_i] \to K$ be the restriction to functions of polynomials in $\mathbb{C}[x_i]$.

Notice that $\ker(\pi_i) \neq 0$ for all i, because otherwise π_i is injective.

Note. For any integral domain with fraction field F any injection $\phi \colon R \to K$ can be extended to an injection $\widetilde{\phi} \colon F \to K$ by $\widetilde{\phi}(a/b) = \phi(a)\phi^{-1}(b)$

(...) ∎

Non-example. $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, so (x^2+1) is maximal in $\mathbb{R}[x]$, but not of the form $X = (x-a)$ because $\mathbb{R}$ is not algebraically closed.

Note. Suppose that $K[x_1, \ldots, x_n]$. Then Hilbert's Nullstellensatz weak form runs into trouble if

1. K is not algebraically closed, (If $\overline{K}$ is the closure of K, then there is a correspondence between maximal ideals in $K[x_1, \ldots, x_n]$ and points in $\overline{K}^n$.) or,
2. if K is countable. (Harder, must use more sophisticated methods.)