Working Over Finite Fields

Gil Cohen

May 26, 2019

Definition

Let K be a field. A polynomial $f(x,y) \in K[x,y]$ is absolutely irreducible if it is irreducible in $\bar{K}[x,y]$.

Definition

We (re)define

$$C_f = K[x,y]/\langle f \rangle$$
$$\bar{C}_f = \bar{K}[x,y]/\langle f \rangle.$$

Discussion

Hilbert's Nullsetellnesatz asserts that if f is absolutely irreducible then

$$Z_f(\bar{K}) \leftrightarrows \mathrm{Max}(\bar{C}_f)$$

In the assignment you will prove that the maximal ideals of C_f correspond still to points of $Z_f(\bar{K})$ though several "conjugated" points together correspond to a single maximal ideal.

Definition

For $(a, b) \in \bar{K} \times \bar{K}$ define

$$\bar{\varphi}_{(a,b)} : \bar{K}[x, y] \to \bar{K}$$

by $g(x, y) \mapsto g(a, b)$.

Let $\varphi_{(a,b)} : K[x, y] \to \bar{K}$ denote the restriction of $\bar{\varphi}_{(a,b)}$ to $K[x, y]$, and let $M_{(a,b)} = \ker(\varphi_{(a,b)})$.

Claim

$$\mathrm{Max}(K[x, y]) = \{M_{(a,b)} \mid (a, b) \in \bar{K} \times \bar{K}\}.$$

Corollary

Let K *be a field and* $f(x,y) \in K[x,y]$ *absolutely irreducible. Let* $M \in \mathrm{Max}(C_f)$. *Then,* $\exists (a,b) \in Z_f(\bar{K})$ *s.t* $M = \ker \psi_{(a,b)}$, *where* $\psi : C_f \to \bar{K}$ *sends* $g(x,y) + C_f \mapsto g(a,b)$.

Corollary

Any $M \in \mathrm{Max}(K[x,y])$ *can be generated by two elements.*

Proof.

There exists $(a, b) \in \bar{K} \times \bar{K}$ such that $M = M_{(a,b)} = \ker(\varphi_{(a,b)})$. Let $g(x) \in K[x]$ be the min poly of a over K. Note that $g(x) \in M$. Write $P = g(x)K[x, y]$. Then,

$$K[x, y]/P \cong (K[x]/g(x))\,[y] \cong K(a)[y]$$

$K(a)$ is a field $\implies K[x, y]/P = K(a)[y]$ is PID. Hence, $\pi_P(M)$ is generated by a single element $h(x, y) + P$ in $K[x, y]/P$. Thus, $M = \langle g(x), h(x, y)\rangle$ □

Claim

Let K be any field. Let $f(x,y) \in K[x,y]$ absolutely irreducible. Let $(a,b) \in Z_f(\bar{K})$ and define

$$\bar{M} = (x-a, y-b)\mathrm{Max}(\bar{C}_f)$$
$$M = \bar{M} \cap C_f.$$

Then, $(\bar{C}_f)_{\bar{M}}$ is a local PID $\implies$ $(C_f)_M$ is a local PID.

Remark

The converse holds if K is a prefect field (and, recall, finite fields are perfect).

Proof.

Since $M \in \mathrm{Max}(C_f)$, $(C_f)_M$ is a local domain. Further, by the above, $\dim((C_f)_M) = 1$. Thus, to prove that $(C_f)_M$ is a PID it suffices to prove that M is principal.

Since $(\bar{C}_f)_{\bar{M}}$ is a local PID, (a, b) is a nonsingular point of $Z_f(\bar{K})$. Assume wlog that $\frac{\partial f}{\partial y}(a, b) \neq 0$.

By the previous claim, $M = \langle g(x), h(x, y) \rangle$. Since $f(x, y) \in M$ there exist $\alpha(x, y), \beta(x, y) \in K[x, y]$ s.t.

$$f(x, y) = \alpha(x, y)g(x) + \beta(x, y)h(x, y).$$

Thus, in $(C_f)_M$:

$$\alpha(x, y)g(x) = -\beta(x, y)h(x, y).$$

□

Proof.

Now,

$$\frac{\partial f}{\partial y}(x,y) = \frac{\partial \alpha}{\partial y}(x,y)g(x) + \frac{\partial \beta}{\partial y}(x,y)h(x,y) + \beta(x,y)\frac{\partial h}{\partial y}(x,y).$$

In particular,

$$0 \neq \frac{\partial f}{\partial y}(a,b) = \beta(a,b)\frac{\partial h}{\partial y}(a,b).$$

Therefore, $\beta(x,y) \notin M$ and so (the class of) $\beta(x,y)$ is a unit in $(C_f)_M$. But recall that in $(C_f)_M$:

$$\alpha(x,y)g(x) = -\beta(x,y)h(x,y).$$

Hence, $M(C_f)_M = g(x)(C_f)_M$. □

Corollary

Let K be any field. Let $f(x,y) \in K[x,y]$ absolutely irreducible. If $Z_f(\bar{K})$ is nonsingular ($\iff$ $\bar{C}_f$ is a Dedekind domain) then C_f is a Dedekind domain.

Remark

The converse holds if K is a prefect field.

Proof of Corollary.

- C_f is a f.g. K-algebra and so by Hilbert's basis theorem, C_f is noetherian.
- We proved that $\dim(C_f) = 1$.

□

Proof.

- We proved that integrally closed is a local property.
  - Every maximal ideal in C_f is of the form $M = \ker(\varphi_{(a,b)})/\langle f \rangle$ for some $(a,b) \in Z_f(\bar{K})$.
  - $(\bar{C}_f)_{\bar{M}}$ is a local PID $\iff$ $(a,b) \in Z_f(\bar{K})$ is nonsingular.

□

Definition

Let L/K be a field extension. The field K is *algebraically closed in* L if every element of L that is algebraic over K is contained in K.

Example

- If K is algebraically closed then it is algebraically closed in any extension L/K.
- Any field K is algebraically closed in $K(x)$.

Theorem

Let K be a perfect field. Let $f(x, y) \in K[x, y]$ irreducible. Then, K is algebraically closed in $K(Z_f) \iff f$ is absolutely irreducible.

Proof.

We'll omit the proof, which requires some field theory work, for lack of time (see Lorenzini VII.4). □