Algebraic Geometric Codes

Recitation 01

Shir Peleg

Tel Aviv University

February 23, 2022

Commutative algebra - Basic definitions

Definition

A *commutative ring with unity* is a set R equipped with two binary operations $\cdot, +$ such that R is abelian in respect to both operators, and there is $1 \in R$ such that for all $x \in R$, $1 \cdot x = x$.

Commutative algebra - Basic definitions

Definition

A *commutative ring with unity* is a set R equipped with two binary operations $\cdot, +$ such that R is abelian in respect to both operators, and there is $1 \in R$ such that for all $x \in R$, $1 \cdot x = x$.

Definition

An *Ideal* in a ring R is a subset $I \subseteq R$, that is a subgroup under addition, and closed under multiplication of any ring element. We denote $I \triangleleft R$.

Commutative algebra - Basic definitions

Definition

A *commutative ring with unity* is a set R equipped with two binary operations $\cdot, +$ such that R is abelian in respect to both operators, and there is $1 \in R$ such that for all $x \in R$, $1 \cdot x = x$.

Definition

An *Ideal* in a ring R is a subset $I \subseteq R$, that is a subgroup under addition, and closed under multiplication of any ring element. We denote $I \lhd R$.

Definition

An ideal $I \lhd R$ is called prime if $\forall a, b \in R \; ab \in I \iff a \in I \vee b \in I$. We denote with $Spec(R)$ the set of all prime ideals in R.

Commutative algebra - Basic definitions

Definition

An ideal $I \triangleleft R$ is called maximal if $I \neq R$ and there is no $J \triangleleft R$ such that $J \neq R$ and $I \subsetneq J$. We denote with $\mathrm{MaxSpec}(R)$ the set of all maximal ideals in R.

Commutative algebra - Basic definitions

Definition

An ideal $I \lhd R$ is called maximal if $I \neq R$ and there is no $J \lhd R$ such that $J \neq R$ and $I \subsetneq J$. We denote with $\mathrm{MaxSpec}(R)$ the set of all maximal ideals in R.

Commutative algebra - Basic definitions

Definition

An ideal $I \triangleleft R$ is called maximal if $I \neq R$ and there is no $J \triangleleft R$ such that $J \neq R$ and $I \subsetneq J$. We denote with $\mathrm{MaxSpec}(R)$ the set of all maximal ideals in R.

Definition

An ideal $I \triangleleft R$ is called principal if there is $r \in R$ such that $I = (r) = \{ar \mid a \in R\} := rR$. A maximal principal ideal is an ideal that is maximal in respect to all principal ideals.

Prime ideals and rings

Claim

P is prime $\iff$ R/P is a domain.

Proof.

We will show that P is not prime $\iff$ R/P is not a domain.

Prime ideals and rings

Claim

P is prime $\iff$ R/P is a domain.

Proof.

We will show that P is not prime $\iff$ R/P is not a domain. P is not prime $\iff$ there are a, b such that $ab \in P$ and $a, b \notin P$ $\iff$ $ab + P = 0, a + P, b + P \neq 0$ in R/P $\iff$ R/P is not a domain. □

Prime ideals and rings

Claim

P is prime $\iff$ R/P is a domain.

Proof.

We will show that P is not prime $\iff$ R/P is not a domain. P is not prime $\iff$ there are a, b such that $ab \in P$ and $a, b \notin P$ $\iff$ $ab + P = 0, a + P, b + P \neq 0$ in R/P $\iff$ R/P is not a domain. □

Home exercise

P is maximal $\iff$ R/P is a field.

Corollary

Every maximal ideal is prime. I.e $\text{MaxSpec}(R) \subseteq Spec(R)$

Filed Extensions – algebraic elements

Definition

Let E/F, b a filed extension. Let $\alpha \in E$, we say that α is algebraic over F if there is a (irreducible) polynomial $p_\alpha \in F[x]$ such that $p_\alpha(\alpha) = 0$.
We say that the extension E/F, is an algebraic extension if all the elements in E are algebraic over F.

MaxSpec of $K[x, y]$

For now assume K is algebraically closed. We want to proof that

$$\text{MaxSpec}(K[x, y]) = \{(x - a, y - b) | a, b \in K\}.$$

Claim

$$\text{MaxSpec}(K[x]) = \{(x - a) | a \in K\}.$$

Proof Sketch

- We show that every ideal in $K[x]$ is principle, i.e generated by on element. Indeed, let $I \triangleleft K[x]$ and let d be a polynomial of minimal degree in I, then $I = (d)$. Proof using euclidean algorithm.

MaxSpec of $K[x, y]$

For now assume K is algebraically closed. We want to proof that

$$\mathrm{MaxSpec}(K[x, y]) = \{(x - a, y - b) | a, b \in K\}.$$

Claim

$$\mathrm{MaxSpec}(K[x]) = \{(x - a) | a \in K\}.$$

Proof Sketch

- We show that every ideal in $K[x]$ is principle, i.e generated by on element. Indeed, let $I \triangleleft K[x]$ and let d be a polynomial of minimal degree in I, then $I = (d)$. Proof using euclidean algorithm.
- $(p) \subseteq (q) \iff q$ divides p.

MaxSpec of $K[x,y]$

For now assume K is algebraically closed. We want to proof that

$$\mathrm{MaxSpec}(K[x,y]) = \{(x-a, y-b) | a, b \in K\}.$$

Claim

$$\mathrm{MaxSpec}(K[x]) = \{(x-a) | a \in K\}.$$

Proof Sketch

- We show that every ideal in $K[x]$ is principle, i.e generated by on element. Indeed, let $I \triangleleft K[x]$ and let d be a polynomial of minimal degree in I, then $I = (d)$. Proof using euclidean algorithm.
- $(p) \subseteq (q) \iff q$ divides p.
- $Spec(K[x]) = \mathrm{MaxSpec}(K[x]) = \{p \in K[x] | p \text{ is irreducible}\}$.

MaxSpec of $K[x, y]$

Claim

$\{(x - a, y - b) | a, b \in K\} \subseteq \mathrm{MaxSpec}(K[x, y])$

MaxSpec of $K[x, y]$

Claim

$\{(x - a, y - b) | a, b \in K\} \subseteq \text{MaxSpec}(K[x, y])$

Proof.

It is enough to show that $K[x, y]/(x - a, y - b)$ is a field. Indeed,

$$K[x, y]/(x - a, y - b) \sim K \text{ via } \varphi(p + (x - a, y - b)) = p(a, b).$$

MaxSpec of $K[x, y]$

Claim

$\{(x-a, y-b) | a, b \in K\} \subseteq \text{MaxSpec}(K[x, y])$

Proof.

It is enough to show that $K[x, y]/(x-a, y-b)$ is a field. Indeed,

$$K[x, y]/(x-a, y-b) \sim K \text{ via } \varphi(p+(x-a, y-b)) = p(a, b).$$

The only thing that we need to show that φ is an injection, i.e if $g(a, b) = 0$ then $g \in (x-a, y-b)$. This can be done using the Taylor expansion of g at the point (a, b). □

Maximal ideals in $K[x, y]$ are not principle

Claim

Let $M \in \text{MaxSpec}(F[x, y])$, *then* M *is not principle.*

Proof.

Consider $I = (f)$ we will show that $I \notin \text{MaxSpec}(F)$.

Maximal ideals in $K[x, y]$ are not principle

Claim

Let $M \in \text{MaxSpec}(F[x, y])$, *then* M *is not principle.*

Proof.

Consider $I = (f)$ we will show that $I \notin \text{MaxSpec}(F)$. We can assume f is irreducible as otherwise the ideal is not prime.

Maximal ideals in $K[x, y]$ are not principle

Claim

Let $M \in \text{MaxSpec}(F[x, y])$*, then* M *is not principle.*

Proof.

Consider $I = (f)$ we will show that $I \notin \text{MaxSpec}(F)$. We can assume f is irreducible as otherwise the ideal is not prime. From Schwartz-Zipple lemma we can show that $\exists a, b \in \overline{F}$ s.t $f(a, b) = 0$ (write $f \in F[x][y]$, choose a non zero value for the coefficient of the leading monomial).

Maximal ideals in $K[x, y]$ are not principle

Claim

Let $M \in \text{MaxSpec}(F[x, y])$, *then* M *is not principle.*

Proof.

Consider $I = (f)$ we will show that $I \notin \text{MaxSpec}(F)$. We can assume f is irreducible as otherwise the ideal is not prime. From Schwartz-Zipple lemma we can show that $\exists a, b \in \overline{F}$ s.t $f(a, b) = 0$ (write $f \in F[x][y]$, choose a non zero value for the coefficient of the leading monomial). We know that in $\overline{F}[x, y]$, both $f, p_a \in (x - a, y - b)$ thus $f, p_a \in (x - a, y - b) \cap F[x, y]$ which is a proper ideal containing f. If we assume that I is maximal we obtain $p_a \in I$. This is a contradiction.

Maximal ideals in $K[x, y]$ are not principle

Claim

Let $M \in \mathrm{MaxSpec}(F[x, y])$, then M is not principle.

Proof.

Consider $I = (f)$ we will show that $I \notin \mathrm{MaxSpec}(F)$. We can assume f is irreducible as otherwise the ideal is not prime. From Schwartz-Zipple lemma we can show that $\exists a, b \in \overline{F}$ s.t $f(a, b) = 0$ (write $f \in F[x][y]$, choose a non zero value for the coefficient of the leading monomial). We know that in $\overline{F}[x, y]$, both $f, p_a \in (x - a, y - b)$ thus $f, p_a \in (x - a, y - b) \cap F[x, y]$ which is a proper ideal containing f. If we assume that I is maximal we obtain $p_a \in I$. This is a contradiction.

Indeed, if $p_a = g \cdot f$ then $f \in F[x]$, which in turn implies that $F[x, y]/(f) = (F[x]/f)[y]$ which is not a field, in contradiction. □

Intersection with $K[x]$

Claim

Let A be a UFD, and M be a non principle ideal in $\operatorname{MaxSpec}(A[x])$ *then* $M \cap A \neq (0)$.

Proof.

Intersection with $K[x]$

Claim

Let A be a UFD, and M be a non principle ideal in $\mathrm{MaxSpec}(A[x])$ *then* $M \cap A \neq (0)$.

Proof.

Assume towards a contradiction that $M \cap A = (0)$. Consider the quotient map:

$$\varphi : A[x] \to A[x]/M := L.$$

Intersection with $K[x]$

Claim

Let A be a UFD, and M be a non principle ideal in $\mathrm{MaxSpec}(A[x])$ *then* $M \cap A \neq (0)$.

Proof.

Assume towards a contradiction that $M \cap A = (0)$. Consider the quotient map:

$$\varphi : A[x] \to A[x]/M := L.$$

From the assumption $\varphi|_A$ is an injection. Denote $K = Frac(A)$. We can extend $\tilde{\varphi} : K[x] \to L$, via $\tilde{\varphi}(\sum \frac{a_i}{b_i} x^i) = \sum \frac{\varphi(a_i)}{\varphi(b_i)} \varphi(x^i)$.

Intersection with $K[x]$

Claim

Let A be a UFD, and M be a non principle ideal in $\mathrm{MaxSpec}(A[x])$ *then* $M \cap A \neq (0)$.

Proof.

Assume towards a contradiction that $M \cap A = (0)$. Consider the quotient map:

$$\varphi : A[x] \to A[x]/M := L.$$

From the assumption $\varphi|_A$ is an injection. Denote $K = Frac(A)$. We can extend $\tilde{\varphi} : K[x] \to L$, via $\tilde{\varphi}(\sum \frac{a_i}{b_i} x^i) = \sum \frac{\varphi(a_i)}{\varphi(b_i)} \varphi(x^i)$. Therefore $M \subseteq Ker(\tilde{\varphi}) = (f_1)$. W.l.o.g. $f_1 \in A[x]$.

Intersection with $K[x]$

Claim

Let A be a UFD, and M be a non principle ideal in $\mathrm{MaxSpec}(A[x])$ *then* $M \cap A \neq (0)$.

Proof.

Assume towards a contradiction that $M \cap A = (0)$. Consider the quotient map:

$$\varphi : A[x] \to A[x]/M := L.$$

From the assumption $\varphi|_A$ is an injection. Denote $K = Frac(A)$. We can extend $\tilde{\varphi} : K[x] \to L$, via $\tilde{\varphi}(\sum \frac{a_i}{b_i} x^i) = \sum \frac{\varphi(a_i)}{\varphi(b_i)} \varphi(x^i)$. Therefore $M \subseteq Ker(\tilde{\varphi}) = (f_1)$. W.l.o.g. $f_1 \in A[x]$. Let $g \in M \subseteq (f_1)$, $f_1 | g$ in $K[x]$

Intersection with $K[x]$

Claim

Let A be a UFD, and M be a non principle ideal in $\mathrm{MaxSpec}(A[x])$ *then* $M \cap A \neq (0)$.

Proof.

Assume towards a contradiction that $M \cap A = (0)$. Consider the quotient map:

$$\varphi : A[x] \to A[x]/M := L.$$

From the assumption $\varphi|_A$ is an injection. Denote $K = Frac(A)$. We can extend $\tilde{\varphi} : K[x] \to L$, via $\tilde{\varphi}(\sum \frac{a_i}{b_i} x^i) = \sum \frac{\varphi(a_i)}{\varphi(b_i)} \varphi(x^i)$. Therefore $M \subseteq Ker(\tilde{\varphi}) = (f_1)$. W.l.o.g. $f_1 \in A[x]$. Let $g \in M \subseteq (f_1)$, $f_1 | g$ in $K[x]$ from Gausses lemma, the same holds in $A[x]$.

Intersection with $K[x]$

Claim

Let A be a UFD, and M be a non principle ideal in $\mathrm{MaxSpec}(A[x])$ *then* $M \cap A \neq (0)$.

Proof.

Assume towards a contradiction that $M \cap A = (0)$. Consider the quotient map:

$$\varphi : A[x] \to A[x]/M := L.$$

From the assumption $\varphi|_A$ is an injection. Denote $K = Frac(A)$. We can extend $\tilde{\varphi} : K[x] \to L$, via $\tilde{\varphi}(\sum \frac{a_i}{b_i} x^i) = \sum \frac{\varphi(a_i)}{\varphi(b_i)} \varphi(x^i)$. Therefore $M \subseteq Ker(\tilde{\varphi}) = (f_1)$. W.l.o.g. $f_1 \in A[x]$. Let $g \in M \subseteq (f_1)$, $f_1 | g$ in $K[x]$ from Gausses lemma, the same holds in $A[x]$. We deduce that $M = (f_1)$ in contradiction. □

MaxSpec($K[x, y]$)

Theorem

$$\mathrm{MaxSpec}(K[x, y]) = \{(x - a, y - b) | a, b \in K\}.$$

Proof.

MaxSpec($K[x, y]$)

Theorem

$$\text{MaxSpec}(K[x, y]) = \{(x - a, y - b) | a, b \in K\}.$$

Proof.

We already showed one inclusion.

MaxSpec($K[x, y]$)

Theorem

$$\text{MaxSpec}(K[x, y]) = \{(x - a, y - b) | a, b \in K\}.$$

Proof.

We already showed one inclusion. For the other direction, let $M \in \text{MaxSpec}(K[x, y])$. From the two previous claims $M \cap K[x] \neq (0)$ thus $M \cap K[x] = (x - a)$.

MaxSpec($K[x, y]$)

Theorem

$$\text{MaxSpec}(K[x, y]) = \{(x - a, y - b) | a, b \in K\}.$$

Proof.

We already showed one inclusion. For the other direction, let $M \in \text{MaxSpec}(K[x, y])$. From the two previous claims $M \cap K[x] \neq (0)$ thus $M \cap K[x] = (x - a)$. Therefore, $(x - a) \subseteq M$,

MaxSpec($K[x, y]$)

Theorem

$$\mathrm{MaxSpec}(K[x, y]) = \{(x - a, y - b) | a, b \in K\}.$$

Proof.

We already showed one inclusion. For the other direction, let $M \in \mathrm{MaxSpec}(K[x, y])$. From the two previous claims $M \cap K[x] \neq (0)$ thus $M \cap K[x] = (x - a)$. Therefore, $(x - a) \subseteq M$, consider $M/(x - a) \in K[x, y]/(x - a) \sim k[y]$.

MaxSpec($K[x,y]$)

Theorem

$$\text{MaxSpec}(K[x,y]) = \{(x-a, y-b) | a, b \in K\}.$$

Proof.

We already showed one inclusion. For the other direction, let $M \in \text{MaxSpec}(K[x,y])$. From the two previous claims $M \cap K[x] \neq (0)$ thus $M \cap K[x] = (x-a)$. Therefore, $(x-a) \subseteq M$, consider $M/(x-a) \in K[x,y]/(x-a) \sim k[y]$. This must be a maximal ideal and thus $M/(x-a) = (y-b)$ Therefore $y - b \in M$, and $M = (x-a, y-b)$. □

MaxSpec(C_f)

Corollary

Let $f \in K[x, y]$ be an irreducible polynomial, then there is a bijection between $Z_f(K)$ and $\text{MaxSpec}(C_f)$ where $C_f = K[x, y]/(f)$.

Proof.

MaxSpec(C_f)

Corollary

Let $f \in K[x,y]$ be an irreducible polynomial, then there is a bijection between $Z_f(K)$ and $\text{MaxSpec}(C_f)$ *where $C_f = K[x,y]/(f)$.*

Proof.

From the third isomorphism theorem, for every $I \in K[x,y]$ $C_f/(I/(f)) = K[x,y]/I$. As there is a correspondence between the ideals of C_f and ideals in $K[x,y]$ that contain (f), we get that $\text{MaxSpec}(C_f) = \{M \in \text{MaxSpec}(K[x,y]) \mid (f) \in M\} = \{(x-a, y-b) \mid f(a,b) = 0\}$. □