Αλγεβρικη Γεωμετρια 23/2/2021

Γεωμετρικα αντικειμενα (Αλγεβρικα συνολα) $\rightsquigarrow$ Αντιμεταθετικοι δακτυλιοι με μονάδα.

Αντιμετ. δακτυλιο $\rightsquigarrow$ Γεωμετρικο αντικειμενο.

M γεωμετρικο αντικειμενο $\rightsquigarrow$ Δακτυλιο των συναρτήσεων $M \to \mathbb{C}$

Αλγεβρικα συνολα

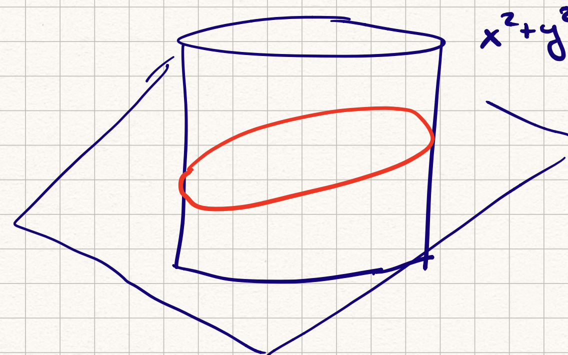
Λυσεις του συστηματος

$$f_\alpha(x_1,\dots,x_n)=0$$

k - σωμα. $\alpha = 1,\dots,\ell$ $\quad f_\alpha \in k[x_1,\dots,x_n]$

$$x^2+y^2=1$$

$$x+y+z=3$$



$$x^3+y^4+xy^6=0$$

$$x+yx^4+\quad=0$$

$\vdots$

$k=\mathbb{C},\mathbb{R}$ $\qquad$ k τυχαιο σωμα, $\to \mathbb{Q}$ Διοφαντικα προβληματα, $\to \mathbb{F}_{p^n}$.

$x^2+y^2=1$ στο $\mathbb{Q}$ $\longrightarrow$ Λυσεις τις πυθαγοριες τριαδες

$x=\frac{\alpha}{\beta}$, $y=\frac{\gamma}{\beta}$ $\quad (\alpha,\gamma,\beta)$ ειναι πυθαγ. τριαδα.

$\mathbb{A}^n_k$ affine variety (ομοπαλληλικα πο/τα)

$= \{(\alpha_1,\dots,\alpha_n)\ \ \alpha_i\in k\}$. $\qquad k^n$ — Διανυσματικο χωρο

f_i συλλογη πολυωνύμων $i\in I$ $\qquad f_i \in k[x_1,\dots,x_n]$

$$V((f_i)_{i\in I}) = \{P=(\alpha_1,\dots,\alpha_n) : f_i(\alpha_1,\dots,\alpha_n)=0\ \ \forall i\in I\}$$

$A = \langle f_i(x_1,\dots,x_n) : i \in I \rangle$ → ιδεωδες που παραγεται απο τα f_i

$$\boxed{g = \sum_{i \in I} g_i(x_1,\dots,x_n) f_i(x_1,\dots,x_n)}$$

$I \lhd R$ ιδεωδες

$(I, +)$ ειναι αβελιανη ομαδα.

$a \cdot f \in I$

$V(A) = \{ P \in A^n_k, \ f(P) = 0 \ \forall f \in A \}$ $\quad \forall a \in R, \forall f \in I.$

$V(A) = V((f_i)_{i \in I})$ $\qquad A \supset \{f_i\}$

$$\boxed{V(\Sigma_1) \supset V(\Sigma_2) \qquad \Sigma_1 \subset \Sigma_2 \subset k[x_1,\dots,x_n]}$$

$V(\Sigma_1)$: ο τοπος μηδενισμου του Σ_1

$V(\Sigma_2)$: τοπος μηδενισμου του Σ_2

$V(A) \subset V((f_i)_{i \in I})$

$P \in V(f_i)_{i \in I}$ τοτε αυτο μηδενιζει καθε $g \in A$

$V(A) \supset V(f_i)$

Παρατηρηση: Αντι να δουμε συλλογες πολυωνυμων αρκει να θεωρούμε ιδεωδη.

(1) $V(0) = A^1_k$ $\qquad \mathbf{0} = \{0\}$

(2) $V(k[x_1,\dots,x_n]) = \emptyset$ $\qquad \forall P \in A^1_k \quad 0(P) = 0$

$c \neq 0 \in k[x_1,\dots,x_n]$

$c(P) = c \neq 0$

Θεώρημα

Βασης Hilbert. $I \lhd k[x_1,\dots,x_n]$ είναι πεπερασμενα παραγμενο.

Δηλαδη υπάρχουν πολυωνυμα $f_1,\dots,f_s$ $\quad I = \langle f_1,\dots,f_s \rangle$

$(f_i)_{i \in I} \longrightarrow I = \langle f_i : i \in I \rangle = \langle f_1,\dots,f_s \rangle$

(ν·ι)ι∈Ι

απειρη οικογενεια πολυωνυμων

πεπερασμενο προβλημα.

Δακτυλιος της Noether ⇒ Καθε αυξουσα ακολουθια ιδεωδων ειναι τελικα σταθερη

$\Updownarrow$

Καθε ιδεωδες ειναι πεπ. παραγομενο.

<u>Εφαρμογή</u>: $k[x_1]$ τοτε καθε ιδεωδες ειναι κυριο παραγεται απο ενα στοιχειο. Αρα τα ιδεωδη του $k[x_1]$ ειναι πεπ. παραγόμενα.

Ο $k[x_1]$ ειναι δακτ. της Noether.

R Noether $\Rightarrow R[x]$ ειναι δακτ. της Noether.

$$k[x_1,\dots,x_n] = \underbrace{k[x_1,\dots,x_{n-1}]}_{n-1}[x_n]$$

$k[x_1,x_2]$ ειναι Noether $\quad k[x_1,x_2] = \overset{R}{(k[x_1])}[x_2]$

<u>Ασκηση</u> Υπαρχουν ιδεωδη του $k[x_1,x_2]$ τα οποια δεν ειναι κύρια.

Απόδ. (Θεωρηματος Βασης)

$\exists$ Α $R[x]$ το οποίο δεν ειναι πεπ. παραγόμενο

$f_0, f_1, \dots, f_n, \dots$ απο πολυωνυμα $\in I$

$\langle f_0 \rangle = b_1 \quad f_1 \notin b_1$

$\langle f_0, f_1 \rangle = b_2 \quad f_2 \notin b_2$

$\vdots$

$\langle f_0,\dots,f_{n-1} \rangle = b_n \quad f_n \notin b_n$

Διαλεγω το $f_n \in I \setminus b_n$ ελαχιστου βαθμο στο συνολο $I \setminus b_n$

$a_n = \mathrm{Lead}(f_n) \longrightarrow$ leading term $\quad f_n = \underline{\underline{a_n}} X^n + a_{n-1} X^{n-1} + \dots$

R Noether

$\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle \subset \dots$

$b = \langle a_0, \dots, a_{N-1} \rangle$ σταθερο ιδεωδες

$\underline{a_N} \in b = \sum_{i<N} u_i a_i$ $\quad u_i \in R$

βαθμου f_i

$g = \sum_{i<N} u_i x^{\deg f_N - \deg f_i} f_i \in R[x]$

πολ. βαθμου f_N $\quad \to a_i$

$\text{Lead}(g) = a_N = \sum_{i<N} u_i a_i$

$a_N x^{\deg f_N} + \dots$

$a_N x^{\deg f_N} + \dots$

$g \in b_N$
$f_N \notin b_N$ $\Rightarrow f_N - g \in b_N$

$\deg(f_N - g) < \deg f_N$ άτοπο

Ορισμό $(I_\lambda)_{\lambda \in \Lambda}$ οικογενεια ιδεωδων.

$\bigcup_{\lambda \in \Lambda} I_\lambda$ δεν είναι ιδεωδες

$\bigcup_{\lambda \in \Lambda} I_\lambda \subset \sum_{\lambda \in \Lambda} I_\lambda$ είναι το ιδεωδες που παραγεται από τα I_λ, $\lambda \in \Lambda$

1) $V(I) \cup V(J) = V(I \cap J)$

2) $\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V\left(\sum_{\lambda \in \Lambda} I_\lambda\right)$

$I \cap J \subset I \Rightarrow V(I) \subset V(I \cap J)$

$V(J) \subset V(I \cap J)$

$V(I) \cup V(J) \subset V(I \cap J)$

$P \in V(I \cap J)$

Αν το $P \in V(I)$ ✓

Υποθετουμε οτι το $P \notin V(I)$

συνεπως υπάρχει $f \in I$ $\quad f(P) \neq 0$

εστω $g \in J$ $\quad h = f \cdot g \in I \cap J$

$$0 = h(P) = \underset{\neq 0}{f(P)} \cdot g(P) \Rightarrow g(P) = 0 \quad \forall g \in J$$

$$\Rightarrow P \in V(J)$$

$f \in I \quad g \in R$
$\Rightarrow f \cdot g \in I$

$f \in R \quad g \in J$
$f \cdot g \in J$

$$I_\mu \subset \bigcup_{\mu \in \Lambda} I_\mu \subset \sum_{\lambda \in \Lambda} I_\lambda$$

$$V(I_\mu) \supset V\Big(\sum_{\lambda \in \Lambda} I_\lambda\Big)$$

$$\bigcap_{\mu \in \Lambda} V(I_\mu) \supset V\Big(\sum_{\lambda \in \Lambda} I_\lambda\Big)$$

Αντιστρόφως $\quad \forall \lambda \in \Lambda \quad I_\lambda = \langle h_{\lambda,1}, \ldots, h_{\lambda,t_\lambda} \rangle$

αφου I_λ ειναι πεπ. παραγ.

$P \in \bigcap_{\mu \in \Lambda} V(I_\mu)$ τοτε

$$h_{\lambda,j}(P) = 0 \qquad \forall \lambda, j \quad \begin{matrix} \lambda \in \Lambda \\ 1 \leq j \leq t_\lambda \end{matrix}$$

Τα $h_{\lambda,j}$ παραγουν το $V\big(\sum_{\lambda \in \Lambda} I_\lambda\big) \Rightarrow P \in V\big(\sum_{\lambda \in \Lambda} I_\lambda\big)$

$$V(I) \cup V(J) = V(I \cap J)$$

Επαγωγικα

$$\bigcup_{j=1}^{s} V(I_j) = V\Big(\bigcap_{j=1}^{s} I_j\Big)$$

Μονο για s πεπερασμενο.

Για απειρες ενωσεις το παραπάνω δεν ισχυει.

Για άπειρες

$c_1,\dots,c_n,\dots$ αριθμήσ. άπειρη συλλογή στοιχείων του άπειρου σώματος k.

$I_j = \langle x-c_j \rangle$ $\qquad V(I_j) = \{c_j\}$

$$I_{j_1} \cap \cdots \cap I_{j_s} = \langle \prod_{i=1}^{s} (x-c_{j_i}) \rangle$$

$$\bigcap_{j=1}^{\infty} I_j = \langle 0 \rangle$$

Ένα πολυώνυμο το οποίο να διαιρείται από από άπειρα διαφορετικά πολυώνυμα.

$$\bigcup_{j=1}^{\infty} V(I_j) = \{c_1,\dots,c_n,\dots\} \subsetneq V\Big(\bigcap_{j=1}^{\infty} I_j\Big) = V(0) = \mathbb{A}^1_k$$

$$\bigcup_{j=1}^{s} I_j = \{c_1,\dots,c_n\} = V\Big(\prod_{i=1}^{s}(x-c_j)\Big)$$

$I \triangleleft R \qquad \sqrt{I} = Rad(I) = \{ f \in R : \exists m \in \mathbb{N} : f^m \in I \}$

Το $\sqrt{I}$ είναι ιδεώδες (άσκηση)

$$\underset{I}{\langle (x^2+y^2-1)^3 \rangle} \rightsquigarrow \sqrt{I} = \langle (x^2+y^2-1) \rangle$$

$$x^2+y^2-1 \notin I \Rightarrow (x^2+y^2-1)^3 \in I$$

$$V(\langle (x^2+y^2-1)^3 \rangle) = V(x^2+y^2-1)$$

Nullstellensatz **Θεώρημα ριζών**

k αλγεβρικά κλειστό σώμα. Αν I με $1 \notin I$ τότε $V(I) \neq \emptyset$

$I = R$ τότε $V(R) = \emptyset$

k δεν είναι αλγεβρικά κλειστό $V(I) = \emptyset$ $\qquad x, y \in \mathbb{R}$, $x^2+y^2 = -1$

Αποδ.

I είναι γνήσιο ιδεώδες του $k[x_1,\dots,x_n]$ συνεπώς υπάρχει ένα μέγιστο ιδεώδες m

$$I \subset m \subsetneq R$$

$V(I) \supset V(m)$ άρα αρκεί να δείξουμε $V(m) \neq \emptyset$ για m μέγιστο.

αλγεβρική επέκταση

$k[x_1,\dots,x_n]/m$ — σώμα, κκ. περιοχή πεπ. παραγόμενη υπέρ το k

k σώμα.

Λήμμα R ακ. περιοχή πεπ. παραγόμενη πάνω από σώμα K και R σώμα. Τότε κάθε στοιχείο του R είναι αλγεβρικό υπέρ το k.

k αλγ. κλειστό $k[x_1,\dots,x_n]/m = k$

$$(x_1 \bmod m, x_2 \bmod m, \dots, x_n \bmod m) = (a_1,\dots,a_n) \in \mathbb{A}^n_k$$

$x_i - a_i \in m \Rightarrow$

$\langle x_1-a_1,\dots,x_n-a_n\rangle \subset m$ $\Rightarrow \langle x_1-a_1,\dots,x_n-a_n\rangle = m$

$\dfrac{k[x_1,\dots,x_n]}{\langle x_1-a_1,\dots,x_n-a_n\rangle} \cong k$ — μέγιστο

$$V(m) = \{(a_1,\dots,a_n)\}$$

Πόρισμα Τα μέγιστα ιδεώδη του $k[x_1,\dots,x_n]$ k αλγεβρικά κλειστό έχουν την μορφή $\langle x_1-a_1,\dots,x_n-a_n\rangle$

k όχι αλγ. κλειστό $\mathbb{Q}[x]$ έχει μέγιστα ιδεώδη $\langle f(x)\rangle$ ανάγωγο

$$\langle x^2-2\rangle$$

Λήμμα R ακ. περιοχή π. παραγόμενη υπέρ το k (όχι υποχρεωτικά αλγεβρικά κλειστό)
R σώμα τότε κάθε στοιχείο του R είναι αλγεβρικό υπέρ το k.

$R = k[z_1,\dots,z_m]$ όλες τις πολυωνυμικές εκφράσεις των $z_1,\dots,z_m$

Αρκεί να δείξουμε ότι τα $z_1,\dots,z_m$ είναι αλγεβρικά υπέρ του k.

<u>Επαγωγή</u> $R = k[z_1]$ $m=1$ αν το z_1 δεν είναι αλγεβρικό υπέρ του k τότε το $k[z_1]$ δεν είναι σώμα. z_1 δεν αντιστρέφεται.

$m \geq 2$. $z_1 \in R$ $k(z_1) \subset R$ υποσώμα

ρητές εκφράσεις του z_1

$R = \underset{\text{σώμα}}{k(z_1)}\underline{[z_2,\dots,z_m]}$ επαγωγική υπόθεση: $z_2,\dots,z_m$ είναι αλγεβρικά υπέρ του $k(z_1)$

$\forall z_j$ $2 \leq j \leq m$ υπάρχει $f_j \in k(z_1)[x]$ που έχει το z_j ως ρίζα.

$$2 \leq j \leq m \quad f_j(x) = \underline{A_j(z_1)}\, x^{n_j} + B_j^{(1)}(z_1)\, x^{n_j-1} + \dots + B_j^{(n_j)}(z_1)$$

$A_j(z_1),\ B_j^{(\ell)} \in \underline{k[z_1]}$

$A(z_1)/A_j(z_1)$

$$A(z_1) = \prod_{j=2}^{m} A_j(z_1)$$

$$S \subset R \qquad k[z_1] \subseteq \underline{S = k\left[z_1, \frac{1}{A(z_1)}\right]}$$

υποδακτύλιος του R (localisation)

$$R = S[z_2,\dots,z_m]$$

$A(z_1)\, x^{n_j} + \dots \in S[z_2,\dots,z_m]$

$x^{n_j} + \dots$ <u>Μονικά</u>

$$g_j(x) = x^{n_j} + b_j^{(1)} x^{n_j-1} + \dots + b_j^{(n_j)}. \quad 2 \leq j \leq m.$$

z_j είναι ακέραιο υπέρ S (ακέραια είναι τα στοιχεία τα οποία ικανοποιούν μονικές αλγεβρικές εξισώσεις

Τα ακέραια στοιχεία υπερ το S που περιέχονται στο R αποτελούν υποδακτύλιο (άσκηση).

Κάθε στοιχείο του R είναι S- ακέραιο.
Αφού το R είναι σώμα θα δείξουμε ότι και το S είναι σώμα.

$a \in S \Rightarrow a^{-1} \in R \Rightarrow a^{-1}$ είναι ρίζα μονικού πολυωνύμου με συντελεστές από το S δηλαδή.

$$a^{-e} + b_1 a^{-e+1} + b_2 a^{-e+2} + \dots + b_e = 0 \qquad b_1, \dots, b_e \in S$$

$$1 + b_1 a + b_2 a^2 + \dots + b_e a^e = 0$$

$$a^{-1} = -(b_1 + b_2 a + \dots + b_e a^{e-1}) \in S$$

Δηλαδή το S είναι σώμα.

Αν το z_1 ήταν υπερβατικό υπερ το k τότε το $\underline{k[z_1]}$ είναι πολ. δακτύλιος υπερ το k

κάθε $a \in K[z_1, \frac{1}{A(z_1)}]$ γράφεται ως

$$a = \frac{F(z_1)}{A(z_1)^s} \qquad F_1(z_1) \in K[z_1]$$

όπ. $F(z_1)$ είναι πρώτο προς το $A(z_1)^s$.

$$a^{-1} = \frac{A(z_1)^m}{F(z_1)}$$ δεν μπορεί να γραφεί ως στοιχείο του S

$$\shortparallel$$

$$\frac{G(z_1)}{A(z_1)^m}$$

$F(z_1)$

$$\frac{G(z_1)}{A(z_1)^m} = \frac{A(z_1)^s}{F(z_1)} \Rightarrow G \cdot F = A(z_1)^{m+s}$$

<u>άτοπο</u>