ΑΛΓΕΒΡΙΚΗ ΓΕΩΜΕΤΡΙΑ

ΜΑΘΗΜΑ 1ο — 30/09

Αλγεβρική Γεωμετρία ήταν αρχικά η μελέτη αλγεβρικών συνόλων

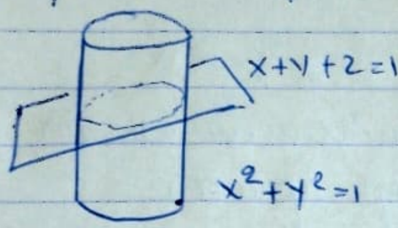
$$f_1(x_1,\dots,x_n), \dots, f_s(x_1,\dots,x_n) \in k[x_1,\dots,x_n]$$

$$\{p \in k^n \mid f_i(p)=0\}$$

Πχ • Αναλυτική Γεωμετρία: $x^2+y^2=1 \rightsquigarrow f(x,y)=x^2+y^2-1$ κύκλος

περιορίζεται σε τετραγωνικές εξισώσεις $\quad \frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1$ ελλειψοειδές

• Συστήματα πολυωνυμικών εξισώσεων στον $\mathbb{R}^3$



Τα κοινά σημεία τους είναι η τομή κυλίνδρου και επιπέδου

Μας ενδιαφέρει η εύρεση των συνόλων

$$V(f_1,\dots,f_s)=\{p\in k^n \mid f_i(p)=0 \ \forall i\}$$

→ Υπάρχουν αλγόριθμοι που απλοποιούν το σύστημα (Βάσεις Gröbner)
Μέθοδοι διαφορικής γεωμετρίας (ανάλυση $k=\mathbb{C}$ ή $\mathbb{R}$)

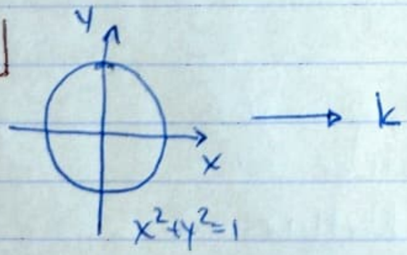
→ Στο μάθημα θα δούμε γεωμετρικά αντικείμενα μελετώντας μέχρι τις συναρτήσεις που ορίζονται σε αυτά

$$V(f_1,\dots,f_n) \longrightarrow k$$

Δημιουργούμε δακτύλιο συναρτήσεων των αλγεβρικών συνόλων

Μελέτη Δακτυλίου ⟶ Μεταθετική Άλγεβρα

Πχ



Θα ορίσουμε $k^2 \xrightarrow{f} k$ πολυώνυμα
Πότε τα $f,g \in k[x,y]$ περιορισμένα στον κύκλο είναι ίδια συνάρτηση?

$$f-g \in (x^2+y^2-1)h(x,y)$$

$$\Leftrightarrow f(p)=g(p) \quad \forall p \in V(x^2+y^2-1)$$

Άρα ο δακτύλιος συναρτήσεων του κύκλου θα είναι ο
$k[x,y]/(x^2+y^2-1)$

Έστω $f_1,\dots,f_s \in R = k[x_1,\dots,x_n]$ και $I = \langle f_1,\dots,f_s\rangle$. $\to$ πεπερ παραγ
Είναι κάθε ιδεώδες του R πεπερ παραγ?
Αν $R=\mathbb{R}[x]$ τότε είναι ΠΚΙ και άρα πεπερ παραγ ιδεώδη

Γιατί μας ενδιαφέρει αυτό? Έχουμε μία αντιστοιχία

$$\begin{array}{ccc} \text{Γεωμετρικό Αντικείμενο} & & \text{Δακτύλιος} \\ \text{Αλγ Σύνολο } V & \longrightarrow & R \\ \operatorname{Spec}\mathbb{Z} & \longleftarrow & \mathbb{Z} \end{array}$$

Πεπερ παραγ ιδεώδες δίνει σύστημα με πεπερ. εξισώσεις

Ορσ. Έστω R μεταθετικός δακτύλιος. Ο R θα λέγεται δακτύλιος της Noether αν ισχύουν οι παρακάτω ισοδύναμες προτάσεις:
1) Κάθε αύξουσα ακολουθία ιδεωδών είναι τελικά σταθερή
2) Κάθε $\neq \emptyset$ σύνολο ιδεωδών έχει μεγιστικό στοιχείο
3) Κάθε ιδεώδες του R είναι πεπερ παραγ

Θεώρημα Βάσης Hilbert: Οι πολυωνυμικοί δακτύλιοι είναι της Noether
R: Noether $\Rightarrow$ $R[x]$ Noether

▸ Ισχύει ότι $V(\langle f_1,\dots,f_n\rangle) = V(f_1,\dots,f_n)$

Σκοπός: Τι γεωμετρικές πληροφορίες του $V(f_1,\dots,f_s)$ αντανακλώνται ως αλγεβρικές πληροφορίες του δακτυλίου αντιστοιχεων $R = k[x,y]/\langle f_1,\dots,f_s\rangle$?

Ορσ Αν $I \trianglelefteq R$, τότε ορίζουμε $V(I) = \{p \in k^n \mid f(p) = 0 \ \forall f \in I\}$

Απόδειξη Θεωρήματος:
Έχουμε ότι $k[x_1,\dots,x_n] = k[x_1,\dots,x_{n-1}][x_n]$, αρκεί νδο
R: Noether $\Rightarrow$ $R[x]$ Noether
Γνωρίζουμε ότι $k[x]$ ΠΚΙ $\Rightarrow$ $k[x]$ της Noether

Έστω $I \trianglelefteq k[x]$ όχι πεπερ. παραγ., τότε $\exists$ αύξουσα ακολουθία ιδεωδών τω $f_i \in I$ και για deg f_{n+1} μικρότερος δυνατός στο $I \setminus I_n$

$$\langle f_1\rangle \subsetneq \langle f_1, f_2\rangle \subsetneq \dots \subsetneq \langle f_1,\dots,f_n\rangle \subsetneq \dots$$

Έστω $a_i = Lt(f_i)$ ο μεγιστοβάθμιος όρος του f_i. Η παραπάνω ακολ. μας δίνει ακολ. από leading terms

$$\langle a_1\rangle \subseteq \langle a_1,a_2\rangle \subseteq \dots \subseteq \langle a_1,\dots,a_n\rangle \subseteq \dots$$

Θδο $\exists N\in\mathbb{N}$ τω η παραπάνω ακολουθία είναι τελικά σταθερή για $n \geq N$, δηλ. $\langle a_1,\dots,a_N\rangle = \langle a_1,\dots,a_N,a_{N+1}\rangle = \langle a_1,\dots,a_{N+1},a_{N+2}\rangle = \dots$

Άρα $\forall n \geq N$ $Lt(f_n) = a_n \in \langle a_1,\dots,a_N\rangle \Rightarrow a_n = \sum_{i=1}^{N} \lambda_i a_i$

Τώρα θέτουμε

$$F = \sum_{i=1}^{N} \lambda_i x^{\deg f_n - \deg f_i} f_i \in \langle f_1,\dots,f_N\rangle$$

και $Lt(F) = Lt(f_n)$

Τότε έχουμε ότι $F \in \langle f_1,\dots,f_N\rangle$ και $f_{N+1} - F \in \langle f_1,\dots,f_{N+1}\rangle$

$f_{N+1} - F \notin \langle f_1,\dots,f_N\rangle$ άτοπο

Καθώς $Lt(F) = Lt(f_n) \Rightarrow f_{N+1} - F$ έχει μικρότερο βαθμό από το f_{N+1} και άρα θα ανήκει αναγκαστικά στο $\langle f_1,\dots,f_N\rangle$. ■

! Ορίζαμε τον χώρο $\mathbb{A}^n_k = \{(a_1,\dots,a_n) \text{ τω } a_i \in k\}$, ο αφινικός χώρος διάστασης n πάνω από το k — σε αντίθεση με το k^n δεν έχει επιπλέον δομή

Κατασκευή #1: Ιδεώδη του $k[x_1,\dots,x_n]$ → Αλγεβρικά Σύνολα

$$I \longmapsto V(I)$$

Κατασκευή #2: Υποσύνολα του $\mathbb{A}^n_k$ → Ιδεώδη του $k[x_1,\dots,x_n]$

$$V \longmapsto I(V) = \{f \in k[x_1,\dots,x_n] \mid f(p)=0 \ \forall p \in V\}$$

(*) Στην πράξη οι I και V είναι αναρτητές.

Ιδιότητες του V: 1) αν $I_1 \subseteq I_2$, τότε $V(I_2) \subseteq V(I_2)$

2) αν $I, J \trianglelefteq k[x_1, \dots, x_n]$, τότε $V(I) \cup V(J) = V(I \cap J)$

3) $\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V(\sum_{\lambda \in \Lambda} I_\lambda)$

4) $\sqrt{I} \subseteq \sqrt{J} \Rightarrow V(I) \supseteq V(J)$

Ορ: Έστω R δακτύλιος και $I \trianglelefteq R$, τότε ορίζουμε το ριζικό του I ως το ιδεώδες (γιατί?) $\sqrt{I} = \{ \alpha \in R \mid \exists n \in \mathbb{N}$ τω $\alpha^n \in I \}$

πχ| $f(x,y) = x^2 + y^2 - 1 \Rightarrow V(x^2+y^2-1)$ κύκλος

$I = \langle f^5 \rangle$, τότε $\sqrt{I} = \langle f \rangle \Rightarrow V(I) = V(x^2+y^2-1)$

θα δούμε ότι $I(V(I)) = \sqrt{I}$

Απόδειξη Ιδιότητες:

1) προφανές

2) $V(I) \subseteq V(I \cap J)$, $V(J) \subseteq V(I \cap J)$ $\Rightarrow V(I) \cup V(J) \subseteq V(I \cap J)$

Έστω $p \in V(I \cap J)$ και $p \notin V(I)$ θδο $p \in V(J)$

$p \notin V(I) \Rightarrow \exists f \in I$ τω $f(p) \neq 0$

Έστω $g \in J$, τότε $gf \in I \cap J \Rightarrow g(p)f(p) = 0 \xRightarrow{f(p) \neq 0} g(p) = 0$

και άρα $p \in V(J)$ $\Rightarrow V(I \cap J) \subseteq V(I) \cup V(J)$. □

Βιβλιογραφία: 1. Grothendieck: EGA, SGA

2. Hartshorne (1977)

3 Mumford (Red Book)

4. R. Vakil: Rising Sea (2022)

5. Ueno: Scheme Theory πάει λίγο τρέχοντας από [illegible]

MAΘHMA 2° 02/10

Συνέχεια Απόδειξης:

3) Ισχύει ότι $I_\lambda \subseteq \Sigma_{\lambda\in\Lambda} I_\lambda \Rightarrow V(\Sigma_{\lambda\in\Lambda} I_\lambda) \subseteq V(I_\lambda)\ \forall \lambda\in\Lambda$

$\Rightarrow V(\Sigma_{\lambda\in\Lambda} I_\lambda) \subseteq \bigcap_{\lambda\in\Lambda} V(I_\lambda)$

Αντίστροφα για κάθε $\lambda\in\Lambda$ γράφουμε $I_\lambda = \langle h_{\lambda 1}, \dots, h_{\lambda t_\lambda}\rangle$ και τότε αν $P\in\bigcap_{\lambda\in\Lambda} V(I_\lambda)$ έχουμε ότι $h_{\lambda,s}(P)=0\ \forall\lambda\in\Lambda\ \forall s\in[t_\lambda]$.

Όμως $V(\Sigma_{\lambda\in\Lambda} I_\lambda) = \langle h_{\lambda k}\rangle \Rightarrow P\in V(\Sigma_{\lambda\in\Lambda} I_\lambda)$, δηλ

$\bigcap_{\lambda\in\Lambda} V(I_\lambda) \subseteq V(\Sigma_{\lambda\in\Lambda} I_\lambda)$

4) Αρκεί νδο $V(I) = V(\sqrt{I})$ (τότε $V(I)=V(\sqrt{I}) = V(\sqrt{J}) = V(J)$)

Προφανώς, $I\subseteq\sqrt{I}$ και άρα $V(\sqrt{I})\subseteq V(I)$.

Έστω τώρα $P\in V(I)$, τότε

$\forall f\in\sqrt{I}\ \ f^m\in I \to f^m(P)=0 \xRightarrow{k \text{ σώμα}} f(P)=0 \Rightarrow P\in V(\sqrt{I})$ ∎

Ορσ: Ένα ιδεώδες $I\trianglelefteq R$ ονομάζεται reduced αν $I=\sqrt{I}$ (ανηγμένο)

αυτό θα δούμε ότι περιέχει πληροφορία στην πολλαπλότητα

Πόρισμα: Έστω $I_1,\dots,I_s\trianglelefteq R$, τότε $\bigcup_{j=1}^s V(I_j) = V(\bigcap_{j=1}^s I_j)$.

⚠ Για άπειρο πλήθος ιδεωδών το παραπάνω δεν ισχύει.

↳ Έστω k άπειρο σώμα και $(c_n)_n$ ακολουθία στο k. διαφορετικά ανά 2

Θεωρούμε τα ιδεώδη $I_j = (x-c_j)$, $j\in\mathbb{N}$, τότε

$I_{j_1}\cap\dots\cap I_{j_s} = \left(\prod_{v=1}^{s}(x-c_{j_v})\right)k[x]$

Από την άλλη έχουμε ότι

$\bigcap_{j=1}^{\infty} I_j = \langle 0\rangle \qquad V(\langle 0\rangle) = \mathbb{A}_k^n$

και άρα

$\bigcup_{j=1}^{\infty} V(I_j) = \bigcup_{n=1}^{\infty}\{c_n\}$ αριθμήσιμο

Άρα δεν γίνεται αν k υπεραριθμήσιμο (πχ. $\mathbb{C}$ ή $\mathbb{R}$) να έχουμε

$\mathbb{A}_k^n = V(\bigcap_{j=1}^{\infty} I_j) = \bigcup_{j=1}^{\infty} V(I_j) = \bigcup_{n=1}^{\infty}\{c_n\}$. ∎

Είχαμε δει την κατασκευή
$$V \subseteq \mathbb{A}^n_k \rightsquigarrow \mathcal{I}(V) = \{f \in R \mid f(p)=0 \ \forall p \in V\}$$
Ας δούμε πως σχετίζονται μεταξύ τους?
αν $V = \mathcal{V}(J)$ για κάποιο $J \trianglelefteq R$, τότε $J \subseteq \mathcal{I}(\mathcal{V}(J))$.
Όμως, έχουμε ότι για $f \in R$
$$\mathcal{V}(\langle f^2 \rangle) = \mathcal{V}(\langle f \rangle) \text{ και } \langle f^2 \rangle \subseteq \mathcal{I}(\mathcal{V}(\langle f^2 \rangle)) = \langle f \rangle.$$
Δεν μπορούμε, λοιπόν, να έχουμε κατ' ανάγκη ισότητα στην παραπάνω σχέση $J = \langle f^2 \rangle$.

Θ. Nullstellensatz: Έστω k αλγεβρικά κλειστό σώμα και $I \trianglelefteq k[x_1,\dots,x_n]$ τω $1 \notin I$, τότε $\mathcal{V}(I) \neq \emptyset$.

⚠ Αν το k δεν είναι αλγεβρικά κλειστό, το παραπάνω δεν ισχύει:
$$x^2+y^2=-1 \quad \text{στο } \mathbb{R} \text{ δεν έχει λύση}$$

Απόδειξη Θεωρήματος:
Έστω $I \ntrianglelefteq R$, τότε $\exists\, m \ntrianglelefteq R$ μέγιστο ιδεώδες τω $I \trianglelefteq m$.
Γνωρίζουμε ότι το $k[x_1,\dots,x_n]/m$ είναι σώμα και περιέχει το k

Λήμμα: Έστω R πεπερ. παραγ. ακέραια περιοχή πάνω από το σώμα k (όχι απαραίτητα αλγ. κλειστό), τότε
$$R \text{ σώμα} \Rightarrow \text{κάθε στοιχείο του } R \text{ είναι αλγεβρικό} / k.$$

Χρησιμοποιώντας το παραπάνω λήμμα έχουμε ότι τα στοιχεία του $k[x_1,\dots,x_n]/m$ είναι αλγ. κλειστό πάνω από το k και k αλγ. κλειστό.
Άρα, $k \simeq k[x_1,\dots,x_n]/m$
Επομένως, $\exists\, \alpha_i \in k$ τω $x_i \equiv \alpha_i \mod m \ \forall i=1,\dots,n$.
Ισχύει ότι $x_i - \alpha_i \in m \Rightarrow J = \langle x_1-\alpha_1,\dots,x_n-\alpha_n \rangle \subseteq m$ και
$k[x_1,\dots,x_n]/\langle x_1-\alpha_1,\dots,x_n-\alpha_n\rangle = k \Rightarrow J$ μέγιστο.
Δηλαδή $J = m$
$$I \subseteq m \Rightarrow \mathcal{V}(I) \supseteq \mathcal{V}(m) = \mathcal{V}(J) = \{(\alpha_1,\dots,\alpha_n)\} \quad \blacksquare$$

Πόρισμα (Ασθενές Nullstellensatz): Έστω L αλγ. κλειστό σώμα, τότε τα μέγιστα ιδεώδη του $L[x_1, \dots, x_n]$ είναι της μορφής $\langle x_1 - a_1, \dots, x_n - a_n \rangle$

(*) Το παραπάνω μας λέει ότι τα σημεία "κωδικοποιούνται" στον $L[x_1, \dots, x_n]$ ως μέγιστα ιδεώδη.

→ επέκταση του R (συμπεριληφθέντα $\in \overline{Quot(R)}$)

Ορ: Έστω $x \in L$, το x ονομάζεται ακέραιο στο R αν ικανοποιεί μονική εξίσωση με συντελεστές από το R

$$x^n + a_{n-1}x^{n-1} + \dots + a_1 x_1 + a_0 = 0$$

Πρόταση: Τα παρακάτω είναι ισοδύναμα για μεταθετικό δακτύλιο R και x σε επέκταση

1. Το x είναι ακέραιο στον R
2. $R[x]$ είναι πεπερασμένα παραγόμενο R-module
3. Υπάρχει πεπερ. παραγ. R-Module τω $xM \subseteq M$.

Απόδειξη:

$1 \to 2$: x ακέραιο $\Rightarrow$ το x ικανοποιεί εξίσωση $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$.

άρα $R[x] = R\langle 1, x, \dots, x^{n-1} \rangle$.

$2 \to 3$: $M = R[x]$

$3 \to 1$: $M = z_1 R + \dots + z_s R$

τότε $x z_1 \in xM \subseteq M \Rightarrow x z_i = \sum_{v=1}^{s} a_{vi} z_v$

$$\Rightarrow x \begin{pmatrix} z_1 \\ \vdots \\ z_s \end{pmatrix} = A \begin{pmatrix} z_1 \\ \vdots \\ z_s \end{pmatrix}$$

$$\Rightarrow (x - I_s A) \begin{pmatrix} z_1 \\ \vdots \\ z_s \end{pmatrix} = 0$$

↳ έχει μη τετριμμένη λύση

$\Rightarrow \det(xI - A) = 0 \Rightarrow x$ ακέραιο

↳ δίνει μονικό χαρακτηριστικό πολ. $x^n + \dots = 0$ ∎

Πόρισμα: Το σύνολο των ακεραίων στοιχείων αποτελεί υποδακτύλιο του $\overline{Quot(R)}$

Απόδειξη:

$$\left.\begin{array}{l} x \text{ ακέραιο} \Rightarrow xM \subseteq M \\ y \text{ ακέραιο} \Rightarrow yN \subseteq N \end{array}\right\} \Rightarrow (x-y)MN \subseteq MN$$

Απόδειξη Λήμματος:

Έστω $R = k[x_1, \dots, x_n]$. Θα εφαρμόσουμε επαγωγή στο n.

Για $n=1$: $R = k[z_1] \to z_1$: αλγεβρικό

$\ker(ev) \longrightarrow K[x] \longrightarrow \bar{K}$

$ev_z : f \longmapsto f(z) \quad Im(ev) = k[z_1] \subseteq E$

αν $\ker(ev) = 0 \Rightarrow z$ υπερβατικό $\Rightarrow k[z_1] \subseteq E$ υποδακτύλιος όχι σώμα

αν $\ker(ev) \neq 0 \Rightarrow z$ αλγεβρικό

παράγεται από 1 πολυώνυμο $k[z] = k[x]/\ker(ev)$ σώμα

$\Leftrightarrow \ker(ev)$ μέγιστο $\Rightarrow$ παράγεται από ανάγωγο

Για $n \geq 2$: Έστω $K(z_1)$ υπόσωμα του R, θεωρούμε

$$R = k(z_1)[z_2, \dots, z_n]$$

Από επαγωγική υπόθεση $z_2, \dots, z_n$ αλγεβρικά στο $K(z_1)$, άρα

$$\exists f_j(x) = A_j(z_1)x^{n_j} + B_j^{(1)}(z_1)x^{n_j-1} + \dots + B_j^{(n_j)}(z_1)$$

όπου $A_j, B_j^{(k)} \in K(z_1)$ $\forall k = 1, \dots, n_j$ έχω A_j για να απαλείψω παρονομαστές

Θέτουμε $A(z_1) = \prod_{j=2}^{n} A_j(z_1)$ και $S = k\left[z, \frac{1}{A(z_1)}\right] \subseteq R$

Έχουμε ότι: $R = S[z_2, \dots, z_m]$ και πολλαπλασιάζοντας την παραπάνω εξίσωση με $A(z_1)/A_j(z_1)$ και διαιρέσουμε με $A(z_1)$ παίρνουμε

$$g_j(x) = x^{n_j} + b_j^{(1)}x^{n_j-1} + \dots + b_j^{(n_j)}$$

μονικό πολυώνυμο με συντελεστές στο $S \Rightarrow z_j$ ακέραιο υπέρ του S.

Τα ακέραια είναι υποδακτύλιος $\Rightarrow$ κάθε $a \in R$ είναι S ακέραιο

Μένει να R σώμα $\Rightarrow S$ σώμα

Έστω $a \in S$, $a \neq 0$, τότε $a^{-1} \in R$ και άρα a^{-1} ρίζα μονικού πολυωνύμου στο S:

$$a^{-\ell} + b_1 a^{-\ell+1} + \dots + b_\ell = 0 \quad , \quad b_i \in S$$

$$\Rightarrow \quad 1 + b_1 a^1 + \dots + b_\ell a^\ell = 0$$

$$\Rightarrow \quad 1 = -(b_1 a^1 + \dots + b_\ell a^\ell)$$

$$\Rightarrow \quad a^{-1} = -(b_1 + b_2 a + \dots + b_\ell a^{\ell-1}) \in S$$

Αν το z_1 ήταν υπερβατικό $/K$, τότε $K[z_1]$ πολυωνυμικός δακτύλιος και $\forall a \in K[z_1, \frac{1}{A(z_1)}]$ ισχύει ότι

$$a = \frac{F(z_1)}{A(z_1)^m} \quad \text{με } F(z_1) \in K[z_1]$$

Μπορούμε να επιλέξουμε το a κατάλληλα, ώστε F και A πρώτα μεταξύ τους, δηλ.

$$\frac{A(z_1)^m}{F(z_1)} = \overset{a^{-1}}{\frac{G(z_1)}{A(z_1)^{\ell}}} \iff A(z_1)^{m+\ell} = F(z_1)G(z_1)$$

Καθώς ο δακτύλιος πολυωνύμων είναι ΠΜΑ $F(z_1) = A(z_1)^{\ell}$ για κάποιο ℓ άτοπο

Σε αυτή την περίπτωση $S = K[z_1, \frac{1}{A(z_1)}]$ όχι σώμα. $\blacksquare$

Θεώρημα (Ισχυρό Nullstellensatz): Αν $J \trianglelefteq K[x_1, \dots, x_n]$ και K αλγεβρικά κλειστό, τότε $\mathcal{I}(\mathcal{V}(J)) = \sqrt{J} \supseteq J$.

Απόδειξη:

$\sqrt{J} \subseteq \mathcal{I}(\mathcal{V}(J))$

$\hookrightarrow f \in \sqrt{J} \Rightarrow f^m \in J \Rightarrow f^m(P) = 0 \quad \forall P \in \mathcal{V}(J)$

$\Rightarrow f(P) = 0 \quad \forall P \in \mathcal{V}(J)$

$\Rightarrow f \in \mathcal{I}(\mathcal{V}(J))$ TBC