Εισαγωγή στην Αλγεβρική Γεωμετρία
Ειδικό Θέμα

Χναράς Φοίβος
Επιβλέπουσα: κ.Χαραλάμπους

10 Μαρτίου 2018

Περιεχόμενα

1 Αφφινικά Αλγεβρικά σύνολα και Αγλεβρικές Ποικιλότητες **9**
1.1 Τοπολογία Zariski . . . 9
1.2 Αλγεβρικά σύνολα και αφφινικοί χώροι . . . 10
1.3 Ανάλυση της Noether . . . 15
1.4 Hilbert 's Nullstellensatz . . . 20
1.5 Αλγεβρικά σύνολα στο Επίπεδο . . . 22

2 Αφφινικές ποικιλότητες **25**
2.1 Δακτύλιοι Συντεταγμένων και Πολυωνυμικές Απεικονίσεις . . . 25
2.2 Ρητές συναρτήσεις, τοπικοί δακτύλιοι και ΔΔΕ . . . 32
2.3 Ευθέα γινόμενα Δακτυλίων . . . 38
2.4 Πράξεις με ιδεώδη . . . 38
2.5 R-modules και ακριβείς ακολουθίες . . . 41

3 Επίπεδες καμπύλες στον Αφφινικό χώρο **45**
3.1 Πολλαπλά σημεία και Εφαπτόμενες Ευθείες . . . 46
3.2 Τοπικοί δακτύλιοι και πολλαπλότητες σημείων . . . 49
3.3 Αριθμοί τομής . . . 53

4 Προβολικές Ποικιλότητες **57**
4.1 Ομογενή Πολυώνυμα . . . 57
4.2 Προβολικός Χώρος . . . 58
4.3 Προβολικά Αλγεβρικά Σύνολα . . . 60
4.4 Αφφινικές και Προβολικές ποικιλότητες . . . 66
4.5 Πολυπροβολικός Χώρος . . . 69

5 Θεώρημα Bezout **73**
5.1 Προβολικές επίπεδες καμπύλες . . . 73
5.2 Θεώρημα Bezout . . . 76

Εισαγωγή

Αυτή η εργασία πρόκειται για μία απλή εισαγωγή στο αντικείμενο της Αλγεβρικής Γεωμετρίας. Αποτελεί κατά το πλείστον περίληψη του βιβλίου του Fulton : Algebraic Curves [Ful89] επιλέγοντας τα σημαντικότερα μέρη από κάθε κεφάλαιο. Τα σχήματα έχουν γίνει με τη βοήθεια των μαθηματικών λογισμικών Geogebra και Mathematica . Πριν ξεκινήσουμε, καλό θα ήταν να έχουμε μία γενική εποπτεία του περί τίνος πρόκειται η αλγεβρική γεωμετρία.

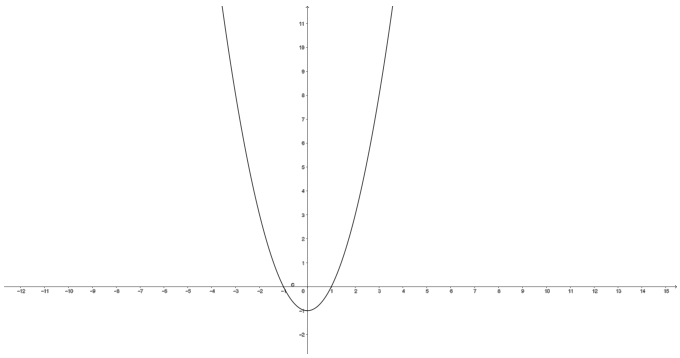
Η Αλγεβρική Γεωμετρία αποτελεί έναν από τους σημαντικότερους κλάδους των μαθηματικών, με πολλά ανοικτά προβλήματα και διαρκή έρευνα. Εάν μπορούσε κανείς να το περιγράψει με μία μόνο φράση, θα έλεγε ότι πρόκειται για την μελέτη των σημείων μηδενισμού ενός συνόλου πολυωνύμων. Το πιο οικείο ίσως παράδειγμα είναι στον δακτύλιο πολυωνύμων $\mathbb{R}[X, Y]$ όπου μπορούμε να μελετήσουμε τα σημεία μηδενισμού ενός ή και παραπάνω πολυωνύμων $f_i(x, y) \in \mathbb{R}[X.Y]$. Το πολυώνυμο $f(x, y) = y - x$ για παράδειγμα έχει ως σημεία μηδενισμού την γνωστή ευθεία στον $\mathbb{R}^2 : y = x$
Γενικεύοντας αυτό το παράδειγμα, θεωρούμε τώρα ως δακτύλιο πολυωνύμων το $k[X_1, ..., X_n]$ όπου k σώμα, και $S = \{f_1(x_1, ..., x_n), ..., f_r(x_1, ..., x_n)\} \subset k[X_1, ..., X_n]$. Ο στόχος τότε είναι η μελέτη του συνόλου

$$V(S) = \{(a_1, ..., a_n) \in k^n = k \times k \times ... \times k : f_i(a_1, ...a_n) = 0 \quad \forall i = 1, ...r\}$$

Στην προσπάθειά μας να περιγράψουμε το σύνολο $V(S)$ θα χρειαστεί να μελετήσουμε αλγεβρικές ιδιότητες του συνόλου πολυωνύμων S το οποίο θα γίνει με τη βοήθεια της Αντιμεταθετικής Άλγεβρας. Η αλγεβρική γεωμετρία συνεπώς δεν πρόκειται παρά μία μετάφραση των αλγεβρικών ιδιοτήτων του S σε γεωμετρικές ιδιότητες του $V(S)$ και αντίστροφα.

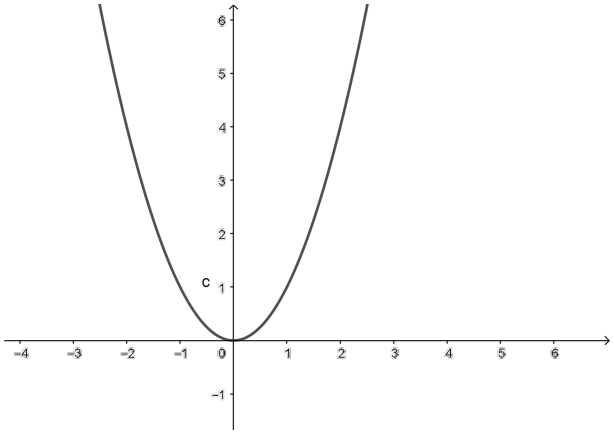
Το κυριότερο εργαλείο λοιπόν της Αλγεβρικής Γεωμετρίας αποτελεί η Αντιμεταθετική Άλγεβρα. Στην παρουσίαση αυτή θα παραθέτουμε κάθε φορά ό,τι θεωρήματα και πορίσματα χρειαζόμαστε από τον τομέα αυτόν, χωρίς όμως να τα αποδυκνείουμε. Για καλύτερη μελέτη των θεωρημάτων αυτών παραπέμπουμε στα βιβλία [Har] και [AM69] . Όλοι οι δακτύλιοι που θα χρησιμοποιούμε θα είναι αντιμεταθετικοί με μονάδα, και πέρα από το πρώτο κεφάλαιο, το k πέρα από σώμα θα το θεωρούμε και αλγεβρικά κλειστό.

Αξίζει να αναφέρουμε λίγα ιστορικά στοιχεία. Η αλγεβρική γεωμετρία είναι ένας σχετικά πρόσφατος κλάδος. Ο λόγος που άργησε τόσο πολύ να αναπτυχθεί είναι επειδή χρειαζόταν την ανάπτυξη δύο βασικών εννοιών: των μιγαδικών αριθμών και των καρτεσιανών συντεταγμένων. Θα μπορούσε κανείς να πει ότι η αλγεβρική γεωμετρία ξεκίνησε με την προσπάθεια για γενίκευση του Θεμελιώδους Θεωρήματος της Άλγεβρας με το οποίο είμαστε όλοι εξοικειωμένοι.
Επιγραμματικά, το Θ.Θ.Α ισχυρίζεται ότι ένα οποιοδήποτε πολυώνυμο βαθμού d έχει ακριβώς d ρίζες. Με την ανάπτυξη των καρτεσιανών συντεταγμένων μπορούμε πια το πολυώνυμο αυτό (π.χ το $y = x^2 - 1$) να το σκεφτούμε ως μία καμπύλη στον χώρο, αλλά και αντίστροφα μία καμπύλη να την μελετήσουμε μέσα από εξισώσεις πολυωνύμων.

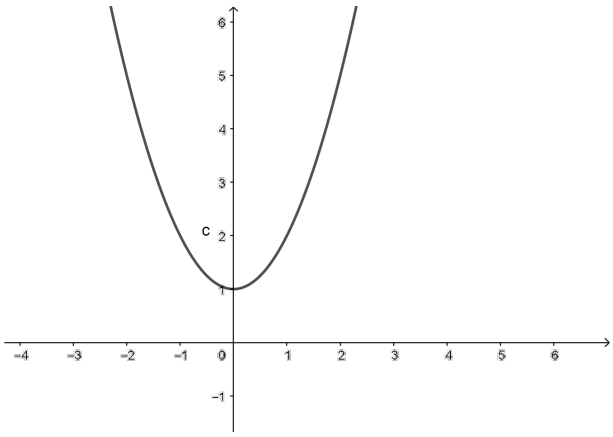


Σχήμα 1

Το Θεώρημα μας λέει απλά ότι η ευθεία $y = 0$ τέμνει την καμπύλη που είναι βαθμού 2 σε 2 σημεία. Βέβαια, έτσι όπως διατυπώθηκε παραπάνω, το θεώρημα είναι ελλιπές και λάθος. Για να έχει οποιοδήποτε πολυώνυμο βαθμού d, d λύσεις, πρέπει να είμαστε σε ένα αλγεβρικά κλειστό σώμα (συνήθως το $\mathbb{C}$). Συνεπώς καταλαβαίνουμε την ανάγκη ύπαρξης των μιγαδικών αριθμών. (Πράγματι, αλλιώς η $y = x^2 + 1$ δεν έχει καμία λύση στο $\mathbb{R}$). Συμβολικά, μας βολεύει να γράφουμε την παραπάνω καμπύλη ως $f(x, y) = y - x^2 - 1$ και ως καμπύλη να εννοούμε πια τα σημεία μηδενισμού του $f(x, y)$. Παρ΄ όλ΄ αυτά, το θεώρημα παραμένει λάθος, καθώς δεν μετρήσαμε την πολλαπλότητα κάθε ρίζας. Για παράδειγμα, λέμε ότι στο $f(x, y) = y - x^2$, (δηλαδή η $y = x^2$) το σημείο $(0, 0)$ έχει πολλαπλότητα 2, ή πιο απλά ότι το 0 είναι διπλή ρίζα του πολυωνύμου.

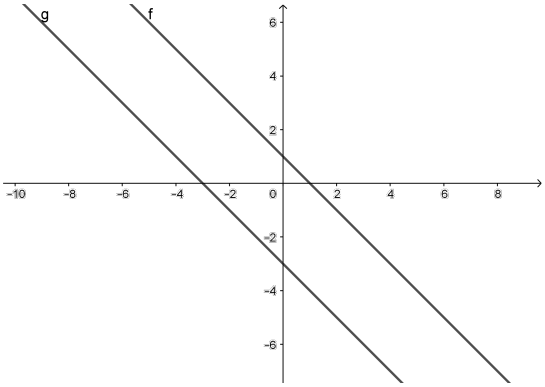


Σχήμα 2: το (0,0) έχει πολλαπλότητα 2



Σχήμα 3: η ευθεία y=0 τέμνει την καμπύλη σε 2 σημεία στον μιγαδικό χώρο

Εν ολίγοις το Θ.Θ.Α μας λέει ότι μία καμπύλη στο μιγαδικό επίπεδο, βαθμού d τέμνει την ευθεία $y = 0$ που είναι βαθμού 1 ($f(x, y) = y$) σε $d \cdot 1$ σημεία. Γιατί όμως να περιοριστούμε στην τομή μιας καμπύλης με μια συγκεκριμένη ευθεία, την $y = 0$; Ο τελικός σκοπός αυτής της εργασίας είναι να γενικεύσουμε αυτό το θεώρημα και να καταλήξουμε ότι δύο οποιεσδήποτε καμπύλες βαθμού m και n αντίστοιχα τέμνονται σε $m \cdot n$ σημεία το οποίο αποτελεί το ξακουστό θεώρημα του Bezout . Εδώ υπάρχουν 2 προβλήματα. Το πρώτο πρόκειται για τα πολλαπλά σημεία, καθώς η πολλαπλότητα ενός σημείου τομής σε 2 τυχαίες καμπύλες δεν είναι κάτι το τόσο προφανές και θα πρέπει να μάθουμε πώς να την υπολογίζουμε. Το δεύτερο και σημαντικότερο πρόκειται για περιπτώσεις όπως οι παράλληλες ευθείες . Τι γίνεται με τις καμπύλες $f(x, y) = x + y - 1, g(x, y) = x + y + 3$;



Σχήμα 4: $y = -x + 1, y = -x - 3$

Αυτές οι 2 καμπύλες, προφανώς δεν τέμνοται ούτε στο πραγματικό αλλά και ούτε στο μιγαδικό επίπεδο, ενώ θεωρητικά είναι βαθμού 1 η κάθε μία οπότε με βάση το θεώρημα θα έπρεπε να τέμνονται σε 1 σημείο. Για τον λόγο αυτό θα εισάγουμε την έννοια του προβολικού χώρου, στον οποίον πλέον αυτές οι ευθείες θα τέμνονται στο άπειρο σε ένα μοναδικό σημείο. Ο χώρος λοιπόν της Αλγεβρικής Γεωμετρίας είναι ο προβολικός, τον οποίο θα μελετήσουμε στα τελευταία κεφάλαια.

Η αλγεβρική γεωμετρία ξεκινάει λοιπόν με δύο μεγάλα ονόματα, τον Gauss (Θ.Θ.Α) και Bezout (θεώρημα Bezout - Γενίκευση του Θ.Θ.Α).

Για μία ενδιαφέρουσα ιστορική αναδρομή παραπέμπουμε σε μία ομιλία του David Eisenbud When the "left-overs" are what counts (David Eisenbud), https://www.youtube.com/watch?v=gi6VZigoJ6U

Κεφάλαιο 1

Αφφινικά Αλγεβρικά σύνολα και Αγλεβρικές Ποικιλότητες

1.1 Τοπολογία Zariski

Όπως αναφέρθηκε και στην εισαγωγή, η αλγεβρική γεωμετρία πρόκειται για μία μετάφραση αλγεβρικών ιδιοτήτων του $S \subset k[X_1, ...X_n]$ σε γεωμετρικές ιδιότητες του $V(S) \subset k^n$. Τις αλγεβρικές ιδιότητες τις μελετάμε μέσω της Αντιμεταθετικής Άλγεβρας.

Γεωμετρία	**Άλγεβρα**
$k^n = k \times k \times .... \times k$	$k[X_1, ..., X_n]$
$V(S)$ $\longleftrightarrow$	S

Για να μελετήσουμε όμως τις γεωμετρικές ιδιότητες του $V(S)$ πρέπει πρώτα να εφοδιάσουμε τον χώρο μας με μία τοπολογία. Η τοπολογία που θα χρησιμοποιηθεί ονομάζεται τοπολογία Zariski και το k^n με την τοπολογία Zariski λέγεται αφφινικός n-χώρος στο k και συμβολίζεται με A_k^n ή $A^n(k)$. Ας θυμηθούμε, όμως, πρώτα τι είναι τοπολογία.

Ορισμός 1.1. *Μία τοπολογία σε ένα σύνολο X είναι μία οικογένεια υποσυνόλων του X με τις εξής ιδιότητες:*

1. *Το X είναι ανοικτό*
2. *Το $\emptyset$ είναι ανοικτό*
3. *Αν $A_i \subset X$ είναι ανοικτά, τότε $\bigcup_i A_i$ είναι ανοικτό (αριθμήσιμη ένωση)*
4. *Αν $A_i \subset X$ είναι ανοικτά, τότε $\bigcap_{i=1}^n A_i$ είναι ανοικτό (πεπερασμένη τομή)*

Στην Αλγεβρική Γεωμετρία μας βολεύει καλύτερα να δουλεύουμε με τα κλειστά σύνολα, οπότε μπορούμε να θεωρήσουμε τα αντίστοιχα αξιώματα για τα κλειστά. Δηλαδή :

Ορισμός 1.2. *Μία τοπολογία σε ένα σύνολο X είναι μία οικογένεια υποσυνόλων του X με τις εξής ιδιότητες:*

1. *Το X είναι κλειστό*
2. *Το $\emptyset$ είναι κλειστό*
3. *Αν $A_i \subset X$ είναι κλειστά, τότε $\bigcap_i A_i$ είναι κλειστό (αριθμήσιμη τομή)*

4. *Αν $A_i \subset X$ είναι κλειστά, τότε $\bigcup_{i=1}^{n} A_i$ είναι ανοικτό (πεπερασμένη ένωση)*

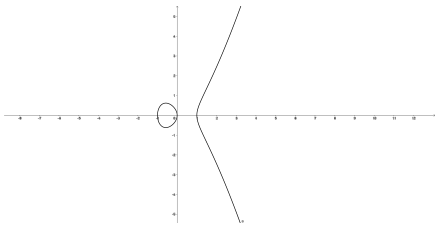
Τότε ταυτίζοντας τα σύνολα $V(S)$ με τα κλειστά σύνολα, προκύπτει η επιθυμητή τοπολογία. Αυτή η ταύτιση θα γίνει πιο αυστηρή στην επόμενη παράγραφο.

1.2 Αλγεβρικά σύνολα και αφφινικοί χώροι

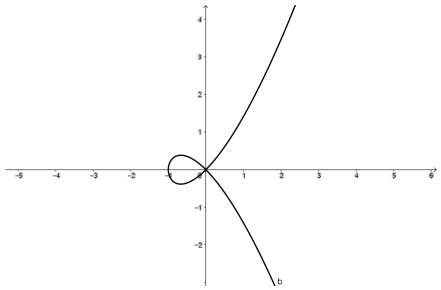
Ξεκινάμε με έναν πολύ βασικό ορισμό.

Ορισμός 1.3. *Ένα υποσύνολο X του A_k^n λέγεται αλγεβρικό εάν υπάρχει σύνολο πολυωνύμων $S \subset k[X_1, ..., X_n]$ τ.ω $X = V(S)$.*

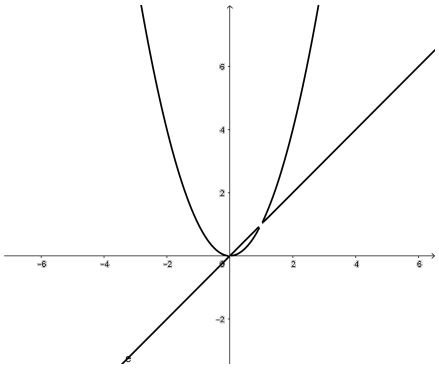
Τα στοιχεία του A_k^n τα ονομάζουμε σημεία, το A_k^1 αφφινική ευθεία και το A_k^2 αφφινικό επίπεδο .
Εάν $F \in k[X_1, ..., X_n]$ μη σταθερό πολυώνυμο τότε το $X = V(F)$ καλείται υπερεπιφάνεια και είναι το σύνολο των μηδενικών (σημείων μηδενισμού) του πολυωνύμου. Μία υπερεπιφάνεια στον A_k^2 καλείται αφφινική επίπεδη καμπύλη. Εάν το F είναι πολυώνυμο πρώτου βαθμού τότε το $V(F)$ καλείται υπερεπίπεδο στο A_k^n και ευθεία για $n = 2$.
Παραδείγματα: Έστω $k = \mathbb{R}$



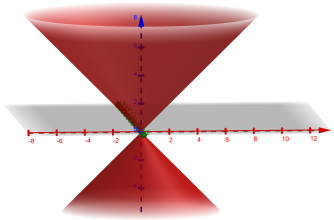
Σχήμα 1.1: α. $V(Y^2 - X(X^2 - 1))$



Σχήμα 1.2: β. $V(Y^2 - X(X^2 + 1))$



Σχήμα 1.3: α. $V(Z^2 - (X^2 + Y^2))$



Σχήμα 1.4: β. $V(Y^2 - XY - X^2Y + Y^3)$

Με τις παρακάτω προτάσεις μπορούμε πλέον να δικαιολογήσουμε γιατί ο χώρος μας είναι τοπολογικός.

Πρόταση 1.1. 1. *$k^n = V(0)$, όπου 0 το μηδενικό πολυώνυμο.*

2. *$\emptyset = V(k[X_1, ..., X_n]) = V(1)$*

3. $V(S_1) \cup ... \cup V(S_m) = V(S_1...S_m)$

4. $\bigcap_a V(S_a) = V(\bigcup_a S_a)$

Απόδειξη. Τα 1 και 2 είναι προφανή.

3 Καταρχάς διευκρινίζουμε τι εννοούμε γράφοντας $S_1...S_m$. Το γινόμενο αυτό ορίζεται ως $S_1...S_m = \{f_1...f_m | f_i \in S_i\}$.
Εάν το σημείο $(a_1, ..., a_n) \in V(S_i)$, δηλαδή $f(a_1, ..., a_n) = 0 \quad \forall f \in S_i$ τότε προφανώς $(a_1, ..., a_n) \in V(S_1...S_m)$, και άρα $V(S_i) \subset V(S_1...S_m) \quad \forall i = 1, ..., m$
$\Rightarrow V(S_1) \cup ... \cup V(S_m) \subset V(S_1....S_m)$.
Ανάποδα, έστω $(a_1, ..., a_n) \in V(S_1...S_m)$.
Εάν $(a_1, ..., a_n) \notin V(S_i)$ για κανένα i τότε αυτό σημαίνει ότι για κάθε i $\exists g_i \in S_i : g_i(a_1, ..., a_n) \neq 0$
Τότε $(g_1....g_m) \in S_1...S_m$, όμως $(g_1...g_m)(a_1, ..., a_n) \neq 0$, που είναι άτοπο.
Συνεπώς $V(S_1....S_m) \subset V(S_1) \cup ... \cup V(S_m)$.

4 Προκύπτει άμεσα από τον ορισμό.
Πράγματι $(a_1, ...a_n) \in \bigcap_i V(S_i) \Leftrightarrow (a_1, ..., a_n) \in V(S_i) \quad \forall i \Leftrightarrow (a_1, ..., a_n) \in V(\bigcup_i S_i)$.

□

Η πρόταση αυτή είναι αρκετά σημαντική, αφού μας λέει ότι το σύνολο k^n γίνεται τοπολογικός χώρος εάν ορίσουμε τα αλγεβρικά υποσύνολα να είναι τα κλειστά. Πράγματι, εύκολα βλέπουμε ότι ικανοποιούνται όλα τα αξιώματα της τοπολογίας. Αυτή η τοπολογία λέγεται τοπολογία Zariski και το k^n με αυτή την τοπολογία συμβολίζεται με A_k^n και ονομάζεται αφφινικός n- χώρος πάνω από το k .

Όπως η μελέτη του γεωμετρικού κομματιού, όπως μόλις είδαμε, γίνεται με τα αλγεβρικά σύνολα, έτσι και το αλγεβρικό κομμάτι μελετάται μέσα από την άλγεβρα και συγκεκριμένα μέσα από τα ιδεώδη.
Καταρχάς πρέπει να θυμηθούμε τι σημαίνει ότι ένα ιδεώδες παράγεται από ένα σύνολο. Θα προσαρμόσουμε τον ορισμό κατευθείαν στο κομμάτι που μας ενδιαφέρει.
Έστω $S \subset k[X_1, ..., X_n]$, ένα σύνολο πολυωνύμων του $k[X_1, ..., X_n]$. Συμβολίζουμε με $I = (S) = \{\sum_i^m f_i g_i | f_i \in S, g_i \in k[X_1, ..., X_n]\}$ το ιδεώδες που παράγεται από το S. Σχετικά εύκολα ελέγχεται ότι το I είναι ιδεώδες και μάλιστα είναι το μικρότερο ιδεώδες τ.ω $S \subset I$. Το σύνολο που γράψαμε παραπάνω, εν τέλει θα προκύψει ότι παράγεται από πεπερασμένο σύνολο στοιχείων (υπό κάποιες προϋποθέσεις) αλλά για να το ισχυριστούμε αυτό χρειαζόμαστε ένα πολύ σημαντικό αποτέλεσμα από την αντιμεταθετική άλγεβρα.
Ξεκινάμε με έναν βασικό ορισμό

Ορισμός 1.4. *Ένας δακτύλιος R καλείται* ***Noetherian*** *εάν κάθε ιδεώδες του είναι πεπερασμένα παραγόμενο.*

Τα σώματα και οι Π.Κ.Ι (περιοχές κυρίων ιδεωδών) είναι προφανές ότι είναι $Noetherian$, αφού στην Π.Κ.Ι κάθε ιδέωδες παράγεται από ένα μόνο στοιχείο, ενώ στο σώμα υπάρχουν μόνο δύο ιδεώδη, το κενό και το ίδιο το σώμα.
Αυτό όμως που χρειαζόμαστε είναι το παρακάτω πολύ σημαντικό θεώρημα

Θεώρημα 1.1 (Θεώρημα βάσης του Hilbert / Θεώρημα της Emmy Noether). *Εάν το R είναι $Noetherian$ τότε το $R[X_1, ..., X_n]$ είναι επίσης $Noetherian$*

Εάν και αποτελεί κομμάτι της Αντιμεταθετικής Άλγεβρας, αξίζει να παραθέσουμε την απόδειξη.

Απόδειξη. Γνωρίζουμε από την Άλγεβρα ότι $R[X_1, ..X_n] \cong R[X_1, ..., X_{n-1}][X_n]$, συνεπώς αρκεί να δείξουμε το θεώρημα για το $R[X]$ και μετά με επαγωγή να το γενικεύσουμε. Έστω λοιπόν ότι R είναι $Noetherian$ και έστω I ένα ιδεώδες στο $R[X]$. Αρκεί να βρούμε ένα πεπερασμένο σύνολο γεννητόρων για το I.
Εάν $F = a_0 + a_1X... + a_dX^d \in \mathbb{R}[X], a_d \neq 0$, τότε ονομάζουμε το a_d *αρχική μεταβλητή* του F. Έστω J το σύνολο όλων των αρχικών μεταβλητών όλων των πολυωνύμων του I. Τότε το J είναι ιδεώδες στο R. Πράγματι, έστω $a, b \in J$, άρα $\exists f, g \in I : f = aX^n + ... + a_1x + a_0, g = bX^m + ... + b_1X + b_0$ και έστω χ.β.γ $n > m$. Τότε, επειδή I ιδεώδες, άρα $h = f - X^{n-m}g \in I$ και το h έχει αρχική μεταβλητή $a - b$, άρα $a - b \in J$. Συνεπώς το J αβελιανή υποομάδα του R. Έστω $a \in J, c \in R$ τότε $\exists f \in I$ τ.ω $f = aX^n + ... + a_1X + a_0$, όμως I ιδεώδες, και άρα $h = cf \in I, h = caX^n + ... + a_0 \Rightarrow ca \in J$. Άρα είναι όντως ιδεώδες
Όμως το R από υπόθεση είναι $Noetherian$ και συνεπώς υπάρχουν πολυώνυμα $F_1, ..., F_m \in I$ που οι αρχικές μεταβλητές τους παράγουν το J. Έστω ένας ακέραιος $N : N > deg(F_i) \forall i = 1, ..., m$. Για κάθε $m \leqslant N$, θεωρούμε J_m ως το σύνολο που αποτελείται από όλες τις αρχικές μεταβλητές όλων των πολυωνύμων $F \in I$ τ.ω $deg(F) \leqslant m$. Το J_m με ίδια διαδικασία όπως πριν δείχνεται εύκολα ότι είναι όντως ιδεώδες για κάθε m. Συνεπώς είναι πεπερασμένο παραγόμενο και άρα μπορούμε να θεωρήσουμε ένα πεπερασμένο σύνολο πολυωνύμων $\{F_{m,j}\} \in I, deg(F_{m,j}) \leqslant m$ των οποίων οι αρχικές μεταβλητές παράγουν το J_m. Έστω I' το ιδεώδες που παράγεται από τα F_i και όλα τα F_{mj}. Προφανώς $I' \subset I$ Αρκεί να δειχτεί ότι $I = I'$.
Έστω ότι $I' \subsetneq I$, και έστω G ένα πολυώνυμο με τον μικρότερο δυνατό βαθμό τ.ω $G \in I - I'$ Εάν $deg(G) > N$, μπορούμε να βρούμε πολυώνυμα Q_i τ.ω $\sum_i Q_iF_i$ έχουν την ίδια αρχική μεταβλητή με το G, αφού οι κυριαρχούμενες μεταβλητές των F_i θεωρήσαμε ότι παράγουν όλο το J. Όμως τότε $deg(G - \sum_i Q_iF_i) < deg(G)$ και άρα $G - \sum_i Q_iF_i \in I'$, αφού το G το διαλέξαμε ώστε ακριβώς να έχει τον χαμηλότερο δυνατό βαθμό. Συνεπώς $G \in I'$.
Όμοια, εάν $deg(G) = m \leqslant N$, μπορούμε να μειώσουμε τον βαθμό αφαιρώντας το $\sum_j Q_jF_{m,j}$ για κάποια Q_j. Αυτό αποδυκνείει το θεώρημα. □

Αφού $S \subset I$ αμέσως συμπεραίνουμε ότι $V(I) \subset V(S)$. Παρόλαυτα ισχύει κατί πολύ πιο ισχυρό που δικαιολογεί την ανάγκη της αντιμεταθετικής άλγεβρας.

Πρόταση 1.2. *Εάν $I = (S)$ και $S \subset k[X_1, ..., X_n]$ τότε $V(I) = V(S)$*

Απόδειξη. Έστω $a = (a_1, ..., a_n) \in V(S)$, άρα $\forall g \in S, \quad g(a_1, ..., a_n) = 0$. Έστω $f \in I = (S) \Rightarrow I = \sum_i g_ih_i, g_i \in S, h_i \in k[x1,, .x_n]$. Τότε προφανώς $f(a_1, ..., a_n) = 0$ και αυτό ισχύει για κάθε $f \in I$, και άρα $a \in V(I)$. □

Η απόδειξη όπως βλέπουμε είναι αρκετά απλή αλλά το αποτέλεσμα είναι αρκετά σημαντικό, αφού μας λέει ότι αρκεί να μελετάμε το ιδεώδες που παράγεται από ένα σύνολο και όχι το σύνολο το ίδιο. Συνεπώς, επόμενος στόχος, είναι η μελέτη αυτών των ιδεωδών και η εύρεση κάποιας αντιστοιχίας μεταξύ αλγεβρικών ιδιοτήτων τους με γεωμετρικές ιδιότητες του $V(I)$.

Καταλήγουμε σε ένα σημαντικό αποτέλεσμα.

Θεώρημα 1.2. *Κάθε αλγεβρικό σύνολο είναι η τομή πεπερασπένου αριθμού υπερεπιφανειών*

Απόδειξη. Έστω V αλγεβρικό σύνολο, άρα υπάρχει $S \subset k[X_1, ..., X_n] : V = V(S)$. Έστω $I = I(S)$. από την προηγούμενη πρόταση $V(S) = V(I)$. Όμως από το Θεώρημα βάσης του Hilbert έχουμε ότι $I = (F_1, ..., F_r)$. Συνεπώς $V(I) = V(F_1, ..., F_r) = V(F_1) \cap ... \cap V(F_r)$ καταλήγοντας στο ζητούμενο. □

Ήδη είμαστε σε θέση να λύσουμε αρκετές βασικές ασκήσεις/προτάσεις της αλγεβρικής γεωμετρίας. Πριν όμως τις δούμε, θα παραθέσουμε, χωρίς απόδειξη κάποιες προφανείς σχέσεις που θα τις χρησιμοποιούμε συχνά από εδώ και εμπρός.

Πρόταση 1.3. *1. Αν $X \subset Y$, τότε $I(X) \supset I(Y)$*

2. *$I(\emptyset) = k[X_1, ..., X_n]$. $I(A_k^n) = (0)$ (αν k άπειρο σώμα).*

3. *$I(\{(a_1, ..., a_n)\}) = (X_1 - a_1, ..., X_n - a_n)$ για $a_i \in k$*

4. *$I(V(S)) \supset S$ για κάθε σύνολο S πολυωνύμων. $V(I(X)) \supset X$ για κάθε σύνολο X σημείων.*

5. *$V(I(V(S))) = V(S)$ για κάθε σύνολο S πολυωνύμων και $I(V(I(X))) = I(X)$ για κάθε σύνολο X σημείων. Συνεπώς, εάν V αλγεβρικό σύνολο, τότε $V = V(I(V))$ και αν I ιδεώδες ενός αλγεβρικού συνόλου, τότε $I = I(V(I))$.*

Στις παρακάτω ασκήσεις/προτάσεις δεν θα θεωρούμε κατ' ανάγκη το k αλγεβρικά κλειστό.

Πρόταση 1.4. *Τα μόνα αλγεβρικά υποσύνολα του A_k^1 είναι τα πεπερασμένα υποσύνολα, μαζί με το A_k^1.*

Απόδειξη. Έστω $X = V(S) \subset A_k^1$. Εάν $S = (0)$, το μηδενικό πολυώνυμο, τότε προφανώς $V(S) = A_k^1$. Αλλιώς, έστω $f \in S, f \neq 0$. Τότε $V(S) \subset V(f)$ (γιατι;) και το f έχει το πολύ $deg(f)$ ρίζες (ακριβώς $deg(f)$ αν το k αλγεβρικά κλειστό), άρα είναι πεπερασμένο. □

Εφαρμογή 1.1. *Είδαμε ότι η πεπερασμένη ένωση αλγεβρικών συνόλων είναι αλγεβρικό σύνολο, ή τοπολογικά η πεπερασμένη ένωση κλειστών είναι κλειστό. Να δώσετε παράδειγμα αριθμήσιμης συλλογής αλγεβρικών συνόλων που η ένωσή τους δεν είναι αλγεβρική.*

Απόδειξη. Θα χρησιμοποιήσουμε την προηγούμενη πρόταση. Έστω $k = \mathbb{C}$ και $V_n = V(X - n) = \{n\}$. Τότε βλέπουμε ότι τα V_n είναι όλα αλγεβρικά και $V_n \subset A^1(\mathbb{C})$. Όμως $\cup V_n = \mathbb{Z}$ το οποίο προφανώς δεν είναι πεπερασμένο και άρα απ την προηγούμενη πρόταση, όχι αλγεβρικό. □

Θέλουμε τώρα να δείξουμε ότι κάθε αλγεβρικά κλειστό σώμα είναι άπειρο, ένα αρκετά σημαντικό αποτέλεσμα που θα το χρησιμοποιούμε συνέχεια παρακάτω παρόλο που δεν θα το αναφέρουμε. Πριν το δείξουμε όμως αυτό, χρειαζόμαστε μία επιπλέον πρόταση/άσκηση:

Πρόταση 1.5. *Έστω k σώμα. Τότε υπάρχουν άπειρα μονικά ανάγωγα πολυώνυμα στο $k[X]$. (Μονικό λέγεται ένα πολυώνυμο που ο αρχικός συντελεστή του είναι 1, δηλαδή είναι της μορφής $f(x) = x^n + a_{n-1}x^{n-1+} + ... + a_1x + a_0$)*

Απόδειξη. Με εις άτοπον. Έστω $F_1, ..., F_n$ όλα τα ανάγωγα μονικά πολυώνυμα και θεωρώ $G = F_1....F_n + 1$. Τότε εύκολα βλέπουμε ότι το G είναι μονικό βαθμού $deg(G) = \sum_i^n F_i$ και συνεπώς είναι σίγουρα διαφορετικό από τα F_i. Αρκεί λοιπόν να δείξουμε ότι είναι ανάγωγο.

Έστω ότι δεν είναι ανάγωγο, άρα υπάρχει ανάγωγο πολυώνυμο H που το διαιρεί. Αν το H δεν είναι μονικό, τότε $H = a_kX^k + ... + a_1X + a_0$ και αφού το k είναι σώμα, άρα το a_k είναι αντιστρέψιμο, και μπορούμε λοιπόν να πολλαπλασιάσουμε με a_k^{-1} ώστε να προκύψει μονικό πολυώνυμο, έστω το H'. Τότε το H' θα είναι μονικό και ανάγωγο, συνεπώς θα ταυτίζεται με ένα από τα F_i. Συνεπώς θα υπάρχει ένα F_i τέτοιο ώστε $F_i|G = F_1...F_n + 1$ που προφανώς είναι άτοπο.

□

Φτάνουμε τώρα στο ζητούμενό μας:

Πρόταση 1.6. *Αν k αλγεβρικά κλειστό τότε είναι άπειρο.*

Απόδειξη. Έστω k πεπερασμένο αλγεβρικά κλειστό σώμα, άρα $k = \{a_1, ..., a + n\}$. Επειδή το σώμα μας είναι αλγεβρικά κλειστό, τα μόνα μονικά ανάγωγα πολυώνυμα είναι της μορφής $F_i = X - a_i$ (γιατί;). Συνεπώς είναι πεπερασμένα σε πλήθος το οποίο είναι άτοπο από την παραπάνω πρόταση.

□

Την επόμενη πρόταση μπορούμε να την χρησιμοποιούμε για να αποδυκνείουμε ότι ένα σύνολο δεν είναι αλγεβρικό.

Πρόταση 1.7. *Έστω C αφφινική επίπεδη καμπύλη και L μία ευθεία στον A_k^2 τ.ω $L \nsubseteq C$. Έστω $C = V(F), F \in k[X,Y]$, με $F[X,Y]$ πολυώνυμο βαθμού n. Τότε $L \cap C$ είναι πεπερασμένο σύνολο, το πολύ n σημείων.*

Απόδειξη. Αφού L ευθεία, έχει εξίσωση της μορφής $Y = aX + b$, άρα $L = V(Y - (aX + b))$ και άρα είναι αλγεβρικό σύνολο. Έστω $F_1 = Y - (aX + b)$
Τότε $L \cap C = V(F) \cap V(Y - (aX + b)) = V(F \cup F_1) = \{(x, y) \in A_k^2 : F(x, y) = 0 \text{και} Y = aX + b\} = V(F(X, aX + b))$.
Όμως $F(X, aX + b) \in k[X]$ και είναι το πολύ n βαθμού (γιατί το πολύ;) άρα έχει το πολύ n λύσεις. □

Μία γρήγορη εφαρμογή για να καταλάβουμε τη χρησιμότητα της παραπάνω πρότασης είναι η εξής :

Εφαρμογή 1.2. *Να δείξετε ότι το παρακάτω σύνολο δεν είναι αλγεβρικό:*
$X = \{(x, y) \in A^2(\mathbb{R}) | y = sin(x)\}$.

Απόδειξη. Αν το X είναι αλγεβρικό, τότε $X = V(S) = \cap_{F \in S} V(F)$ για κάποιο $S \subset \mathbb{R}[X,Y]$. Θεωρούμε την ευθεία $L = \{(x, y) \in A^2(\mathbb{R}) | y = 0\}$, δηλαδή των άξονα των x. Προφανώς $L \nsubseteq X$ αφού για παράδειγμα $(\frac{\pi}{2}, 0) \in L$ ενώ $(\frac{\pi}{2}, 0) \notin X$. Παίρνουμε ένα πολυώνυμο $F \in S$. Τότε $X \subset V(F)$ είναι αφφινική επίπεδη καμπύλη και $L \nsubseteq V(F)$. Από την προηγούμενη όμως πρόταση συμπεραίνουμε ότι $L \cap V(F) \supseteq L \cap X = \{(k\pi, 0) | k \in \mathbb{Z}\}$ είναι πεπερασμένο σύνολο που είναι άτοπο. Συνεπώς X όχι αλγεβρικό. □

Η επόμενη πρόταση/άσκηση μας δίνει μία γεωμετρική διαίσθηση για τα αλγεβρικά σύνολα και τα συμπληρώματά τους.

Πρόταση 1.8. *Έστω F ένα μη σταθερό πολυώνυμο στο $k[X_1, ..., X_n]$, k αλγεβρικά κλειστό. Τότε $A_k^n - V(F)$ είναι άπειρο, αν $n \geq 1$ και $V(F)$ είναι άπειρο αν $n \geq 2$. Συμπεραίνουμε λοιπόν ότι το συμπλήρωμα κάθε αλγεβρικού συνόλου είναι άπειρο.*

Απόδειξη. Θα χρειαστούμε ένα απλό γεγονός από την άλγεβρα που θα το χρησιμοποιήσουμε χωρίς απόδειξη: Αν k είναι άπειρο σώμα και $F \in k[X_1, ..., X_n]$, τότε εάν $F(a_1, ..., a_n) = 0 \quad \forall (a_1, ..., a_n) \in A_k^n$ τότε $F \equiv 0$ (η απόδειξη προκύπτει εύκολα με επαγωγή στο n).
Γυρνάμε τώρα στο πρόβλημα. Καταρχάς αφού k αλγεβρικά κλειστό έχουμε από την πρόταση 1.6 ότι είναι άπειρο, άρα και το A_k^n είναι άπειρο.
Αν $A_k^n - V(F)$ πεπερασμένο, τότε $\exists J \subseteq k[X_1, ..., X_n]$ τ.ω $A_k^n - V(F) = V(G) \Rightarrow A_k^n = V(F) \cup V(J)$ όπου $J = I(G_1, ..., G_s)$ ιδεώδες.
Όμως $V(F) \cup V(J) = V(FJ) = A_k^n = V(0)$. Συνεπώς για κάθε $G \in J$, $(FG)(a_1, ..., a_n) = 0 \forall (a_1, ..., a_n) \in A_k^n$. Από την προηγούμενη όμως πρόταση συμπεραίνουμε ότι $FG \equiv 0$ και επειδή είμαστε σε ακεραία περιοχή (γιατί;), άρα $F \equiv 0$ ή $G \equiv 0$. Όμως F όχι σταθερό από υπόθεση, άρα $J = (0)$. Συνεπώς $V(J) = A_k^n$ και άρα όχι πεπερασμένο που είναι άτοπο. Συνεπώς $A_k^n - V(F)$ είναι άπειρο για κάθε $n \geq 1$
Αν $n \geq 2$ τότε $V(F) = \{P \in A_k^n : F(P) = 0\}$. Γράφουμε το F ως $F = \sum F_i X_n^i, F_i \in k[X_1, ..., X_{n-1}]$. Έχουμε 2 περιπτώσεις
(α): F_i σταθερό για κάθε i, δηλαδή $F \in k[X_n]$ και συνεπώς προφανώς $V(F)$ είναι άπειρο (επειδή το σώμα μας είναι αλγεβρικά κλειστό) (γιατί;).
(β): Υπάρχει κάποιο μη σταθερό F_i. Συνεπώς $A_k^{n-1} - V(F_i)$ είναι άπειρο, αφού υπάρχουν άπειρα σημεία $(a_1, ..., a_{n-1})$ τέτοια ώστε $F_i(a_1, ..., a_n) \neq 0$ (γιατι;!). Για κάθε τέτοιο σημείο έχουμε ότι $F(a_1, .., a_{n-1}, X_n) \in k[X_n]$ και αφού k αλγεβρικά κλειστό, μπορούμε να βρούμε $a_n \in k : F(a_1, ..., a_n) = 0$. Συνεπώς $V(F) \supset \{(a_1, ..., a_{n-1}, a) | F_i(a_1, ..., a_{n-1}) \leq 0\}$ είναι άπειρο.

Το τελευταίο ερώτημα προκύπει άμεσα αν θεωρήσουμε $S \subset k[X_1, ..., X_n]$ και $F \in S$, τότε το αλγεβρικό σύνολο είναι της μορφής $X = V(S) \subset V(F) \Rightarrow A_k^n - V(S) \supset A_k^n - V(F)$.
Να παρατηρήσουμε ότι σε όλη την πρόταση υποθέσαμε ότι το αλγεβρικό σύνολο είναι γνήσιο υποσύνολο του A_k^n, Προφανώς αν $F \equiv 0$ τότε δεν ισχύουν τα παραπάνω.

□

Οι επόμενες ασκήσεις/προτάσεις είναι κυρίως αλγεβρικές αλλά πολύ βασικές για τα παρακάτω.

Πρόταση 1.9. *Έστω k σώμα και $F \in k[X_1, ..., X_n]$, $a_1, ..., a_n \in k$. Τότε ισχύουν τα εξής :*

1. $F = \sum_{i=0} r_i(X_1 - a_1)^{i_1} \cdot ... \cdot (X_n - a_n)^{i_n}$, $r_i \in k$
2. *Αν $F(a_1, ..., a_n) = 0$ τότε $F = \sum_{i=1}^{n}(X_i - a_i)G_i$ για κάποιο $G_i \in k[X_1, ..., X_n]$ (όχι μοναδικό).*

Απόδειξη. 1. Θα το δείξουμε με επαγωγή στο n.
Για $n = 1$ έχουμε $F[X] = b_nX^n + ... + b_1X + b_0$ και έστω $a \in k$. Επειδή είμαστε σε ευκλείδια περιοχή μπορούμε να κάνουμε επαναλαμβανόμενες διαιρέσεις με το $X - a$ και να προκύψει η ζητούμενη μορφή.
Έστω ότι ισχύει για $n - 1$ και έστω $F \in k[X_1, ..., X_n]$ και $a_1, ..., a_n \in k$. Τότε $F \in k[X_1, ..., X_{n-1}][X_n]$ άρα μπορώ να γράψω το F ως $F = \sum_{i=0} G_i(X_n - a_n)^i$, όπου $G_i \in k[X_1, ..., X_{n-1}]$. Στα G_i μπορώ να εφαρμόσω την υπόθεση επαγωγής και να προκύψει το ζητούμενο.

2. Αν $F(a_1, ..., a_n) = 0$ και από το προηγούμενο έχουμε ότι $F = \sum_{i=0} r_i(X_1 - a_1)^{i_1} \vdots ... \cdot (X_n - a_n)^{i_n}$, $r_i \in k$, τότε προφανώς ο σταθερός όρος του πολυωνύμου είναι 0, δηλαδή $r_i = 0$ όταν $i_1, ..., i_n = 0$ και άρα κάθε όρος του F μπορεί να γραφεί ως $F_i = (X_i = a_i)[r_i(X_1 - a_1)^{i_1} ... (X_{i-1} - a_{i-1})^{i_{i-1}} ... (X_n - a_n)^{i_n}]$. Θέτοντας απλά $G_i = [r_i(X_1 - a_1)^{i_1} ... (X_{i-1} - a_{i-1})^{i_{i-1}} ... (X_n - a_n)^{i_n}$ έχουμε τη ζητούμενη μορφή.

□

Πρόταση 1.10. *Έστω k άπειρο σώμα. Τότε τα μέγιστα ιδεώδη στον $k[X_1, ..., X_n]$ είναι της μορφής $M = (X_1 - a_1, , , X_n - a_n)$. Αν $(a_1, ..., a_n) \in A_k^n$ τότε $I(\{(a_1, ..., a_n)\}) = (X_1 - a_1, ..., X_n - a_n)$.*

Πέρα από το αποτέλεσμα, η μεθοδολογία της απόδειξης είναι αρκετά βασική.

Απόδειξη. Έστω $M = (X_1 - a_1, , , X_n - a_n)$.
Για να δείξουμε ότι ένα ιδεώδες είναι μέγιστο, θυμίζουμε από την αντιμεταθετική άλγεβρα ότι αρκεί να δείξουμε ότι ο δακτύλιος πηλίκο $k[X_1, ..., X_n]/M$ είναι σώμα (αντίστοιχα ακεραία περιοχή για τα πρώτα ιδεώδη). Έστω, λοιπόν $R = k[X_1, ..., X_n]/M$ ο δακτύλιος πηλίκο και $f \in R$. Τότε $f = F + R$, $f \in k[X_1, ..., X_n]$. Όμως από την προηγούμενη πρότασηση έχουμε ότι κάθε F μπορεί να γραφεί στην μορφή $F = \sum_{i=0} r_i(X_1 - a_1)^{i_1} \cdot ... \cdot (X_n - a_n)^{i_n}$, $r_i \in k$. Αν με r_0 συμβολίσουμε την περίπτωση όπου $i_1 = ... = i_n = 0$ και F_0 τον αντίστοιχο όρο του F τότε παίρνοντας το F μέσα στο R έχουμε ότι $f = r_0 + R$, $r_0 \in k$. Προφανώς $F \in M \Leftrightarrow r_0 = 0 \Leftrightarrow f = 0$. Αν $F \notin M \Rightarrow r_0 \neq 0 \Rightarrow f = r_0 + R \neq 0_R$. Όμως k σώμα άρα r_0 αντιστρέψιμο, άρα f αντιστρέψιμο και άρα R σώμα. Συνεπώς, πράγματι M μέγιστο ιδεώδες . Για να δείξουμε το δεύτερο ζητούμενο αρκέι να παρατηρήσουμε ότι $M \subset I(V) = I(\{(a_1, ..., a_n)\})$ και $I(V)$ γνήσιο ιδεώδες (αφού k άπειρο σώμα). Συνεπώς, αφού M μέγιστο ιδεώδες άρα $I(V) = M$. □

1.3 Ανάλυση της Noether

Στα πολυώνυμα λέμε ότι το F είναι ανάγωγο, αν υπάρχουν μη σταθερά G, H πολυώνυμα τ.ω $F = GH$. Θα δούμε ότι υπάρχει ένας παρόμοιος γεωμετρικός ορισμός στα αλγεβρικά σύνολα

Ορισμός 1.5. *Ένα αλγεβρικό σύνολο V λέγεται αναλύσιμο εάν υπάρχουν υποσύνολα $V_1, V_2 \in A^n$, αλγεβρικά, με $V_i \neq V, i = 1, 2$ τ.ω $V = V_1 \cup V_2$. Αλλιώς λέγεται **ανάγωγο** (irreducible).*

Πρόταση 1.11. *Ένα αλγεβρικό σύνολο V είναι ανάγωγο αν-ν $I(V)$ είναι πρώτο ιδεώδες.*

Απόδειξη. Έστω $I(V)$, όχι πρώτο, δηλαδή υπάρχουν $F_1F_2 \in I(V), F_i \notin I(V)$. Έστω $V_1 = V \cap V(F_1), V_2 = V \cap V(F_2)$. Τότε $(F_1F_2) \subset I(V) \Rightarrow V \subset V(F_1F_2) = V(F_1) \cup V(F_2) \Rightarrow V = V \cap (V(F_1) \cup V(F_2) = V_1 \cup V_2$. Όμως $V \cap V(F_i) \subsetneqq V$, αφού $F_i \notin I(V)$ και άρα V είναι αναλύσιμο που είναι άτοπο.
Ανάποδα, εάν $V = V_1 \cup V_2, V_i \subsetneqq V$, τότε $I(V_i) \supsetneqq I(V)$. Έστω $F_i \in I(V_i), F_i \notin I(V)$. Τότε $F_1F_2 \in I(V)$ (γιατί;) και άρα $I(V)$ όχι πρώτο. □

Επόμενος στόχος είναι να γράψουμε τα αναλύσιμα σύνολα ως ενώσεις αναγώγων συνόλων και όχι απλά αλγεβρικών. Σκοπός μας είναι να δείξουμε ότι αυτή η ένωση θα είναι πεπερασμένη. Δηλαδή εάν V αναλύσιμο, γράφουμε $V = V_1 \cup V_2$. Αν το V_2 είναι με τη σειρά του αναλύσιμο συνεχίζουμε και γράφουμε $V_2 = V_3 \cup V_4$. Θέλουμε να δείξουμε ότι αυτή η διαδικασία κάποια στιγμή σταματάει.

Πρόταση 1.12. *Έστω S μία μη κενή συλλογή ιδεωδών σε έναν Noetherian δακτύλιο. Τότε το S έχει μεγιστικό στοιχείο, δηλαδή υπάρχει ιδεώδες $I \in S$ τ.ω να μην περιέχεται σε κανένα άλλο ιδεώδες του S.*

Απόδειξη. Θα χωρίσουμε διαδοχικά το S σε υποσύνολα. Ξεκινάμε διαλέγοντας αυθαίρετα ένα ιδεώδες $I_0 \in S$. Θεωρούμε το υποσύνολο $S_1 = \{I \in S | I \supsetneqq I_0\}$ και έστω $I_1 \in S_1$. Τότε θεωρούμε πάλι $S_2 = \{I \in S | I \supsetneqq I_1\}$. Αρκεί να δείξω ότι σε κάποιο βήμα $n < \infty$ το S_n θα είναι κενό. Έστω ότι δεν είναι. Τότε θέτουμε $I = \bigcup_{n=1}^{\infty} I_n$, το οποίο είναι ιδεώδες του R. Να παρατηρήσουμε ότι εν γένει η ένωση ιδεωδών δεν είναι πάντα ιδεώδες, αλλά εδώ που τα I_n έχουν σχέση εγκλεισμού ισχύει (η απόδειξη είναι αρκετά απλή).
Αφού είμαστε σε Noetherian δακτύλιο, το I είναι πεπερασμένα παραγόμενο, άρα $I = (F_1, ..., F_r)$. Όμως εξ ορισμού $F_i \in I \Rightarrow \exists n \in \mathbb{N} : F_i \in I_n$. Διαλέγοντας το μέγιστο από αυτά τα n (μπορούμε γιατί F_i πεπερασμένα) και ας το συμβολίσουμε με N, τότε $F_i \in I_N \forall i = 1, .., r$. Συνεπώς $I = I_N$, και άρα $I_{N+1} = I_N$ που είναι άτοπο από υπόθεση. □

Αυτή η πρόταση μας απαντάει αμέσως το προηγούμενο πρόβλημα που θέσαμε. Δηλαδή, κάθε συλλογή αλγεβρικών συνόλων στο A_k^n έχει ελαχιστικό στοιχείο. Πράγματι, αν $\{V_a\}$ μία τέτοια συλλογή και περάσουμε στα ιδεώδη που παράγονται από αυτά τα σύνολα, τα $\{I(V_a)\}$, τότε από την πρόταση, υπάρχει κάποιο στοιχείο $I(V_{a_0})$ από το $\{I(V_a)\}$ που να είναι μεγιστικό. Πηγαίνοντας πίσω στον αφφινικό χώρο, βλέπουμε αμέσως ότι το V_{a_0} είναι ελαχιστικό.
Το αποτέλεσμα αυτό μας δείχνει ότι ένα αναλύσιμο αλγεβρικό σύνολο αναλύεται σε πεπερασμένα ανάγωγα σύνολα, αλλά όπως θα δούμε ισχύει κάτι πολύ πιο ισχυρό.

Θεώρημα 1.3 (Ανάλυση της Noether (Noetherian Decomposition)). *:*
Έστω $V \subset A_k^n$ ένα αλγεβρικό σύνολο. Τότε υπάρχουν <u>μοναδικά</u> σύνολα $V_1, ..., V_m$ τ.ω $V = V_1 \cup ... \cup V_m$ και $V_i \not\subseteq V_j \forall \quad i \neq j$.

Πριν το αποδείξουμε θα χρειαστούμε το επόμενο λήμμα.

Πρόταση 1.13. *Αν $V = V_1 \cup V_2 \cup ... \cup V_r$ όπου V ανάγωγο και V_i αλγεβρικά, τότε $V \subset V_i$ για κάποιο i.*

Απόδειξη. Το V μπορούμε να το γράψουμε ως $V = (V \cap V_1) \cup (V \cap V_2) \cup ... \cup (V \cap V_r)$. Κάθε $V \cap V_i$ είναι κλειστό. Υποθέτουμε ότι $V \cap V_i \neq \emptyset \forall i$, αλλιώς απλά το πετάμε απέξω.
Αν κάποιο $V \cap V_i = V$ τελειώσαμε.
Έστω ότι $V \cap V_i \subsetneqq V$. Τότε $V = (V \cap V_1)[\cup (V \cap V_2) \cup ... \, cup (V \cap V_r)]$ όπου $(V \cap V_1), [\cup (V \cap V_2) \cup ... \, cup (V \cap V_r)]$ μη κενά γνήσια αλγεβρικά υποσύνολα. Συνεπώς V όχι ανάγωγο, άτοπο. □

Περνάμε στην απόδειξη του θεωρήματος.

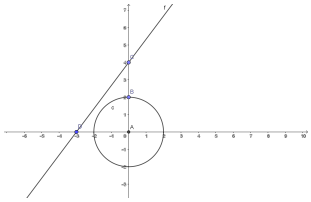
Απόδειξη. Την ύπαρξη την έχουμε πρακτικά δείξει.
Έστω $S = \{$αλγεβρικά σύνολα $V \subset A^n_k | V$δεν γράφεται ως ένωση πεπερασμένου αριθμού αναγώγων συνόλων$\}$. Θέλουμε να δείξουμε ότι $S = \emptyset$. Έστω οτι δεν είναι. Από την προηγούμενη πρόταση υπάρχει V ελαχιστικό στοιχείο του S. Αφού $V \in S$ άρα V όχι ανάγωγο, συνεπώς υπάρχουν γνήσια αλγεβρικά υποσύνολα ώστε $V = V_1 \cup V_2, V_i \subsetneq V$. Τότε, αφού V ελαχιστικό, συνεπώς $V_i \notin S$ και άρα το V_i αναλύεται σε πεπερασμένο πλήθος αναγώγων αλγεβρικών υποσυνόλων $V_i = V_{i1} \cup ... \cup V_{im_i}$ με V_{ij} ανάγωγα. Όμως τότε $V = \bigcap_{i,j} V_{ij}$ που είναι άτοπο.
Συνεπώς κάθε V αλγεβρικό μπορεί να γραφεί ως $V = V_1 \cup ... \cup V_m$, V_i ανάγωγα. Για να επιτύχουμε τη μοναδικότητα απλά πετάμει όσα V_i είναι υποσύνολα άλλων V_j, δηλαδή όσα $V_i \subset V_j$ για κάποια i, j . Υποθέτουμε λοιπόν χωρίς βλάβη της γενικότητας ότι $V = V_1 \cup ... \cup V_m$, V_i ανάγωγα και $V_i \nsubseteq V_j$ για κανένα i, j.Για να δείξουμε την μοναδικότητα υποθέτουμε ότι $V = W_1 \cup ... \cup W_n$ μία δεύτερη ανάλυση. Τότε $V_i = V \cap V_i = \bigcup_{j=1}^n W_j \cap V_i = \bigcup_{j=1}^n (W_j \cap V_i)$, δηλαδή $V_i \subset W_{j(i)}$ για κάποιο $j(i)$ από την προηγούμενη πρόταση. Όμοια έχουμε ότι $W_{j(i)} \subset V_k$ για κάποιο k . Όμως $V_i \subseteq V_k \Leftrightarrow i = k$, και άρα $V_i = W_{j(i)}$. Όμοια κάθε W_j ισούται με κάποιο $V_{i(j)}$. □

Αυτά τα V_i ονομάζονται **ανάγωγοι παράγοντες (irreducible components)** του V. Η ανάλυση του V ως $V = V_1 \cup ... \cup V_m$ λέγεται **Ανάλυση της Noether Noetherian Decomposition** του V σε ανάγωγους παράγοντες. Ένα αφφινικό αλγεβρικό ανάγωγο σύνολο ονομάζεται αφφινική ποικιλότητα (affine variety).
Αυτό το θεώρημα μας δείχνει πόσο σημαντικές είναι οι αφφινικές ποικιλότητες οι οποίες είναι στην ουσία οι οικοδομικοί λίθοι, όχι μόνο στην αλγεβρική γεωμετρία που μελετάμε εδώ, αλλά και στο scheme theory που είναι η μελέτη της αλγεβρικής γεωμετρίας όταν το σώμα μας δεν είναι αλγεβρικά κλειστό.

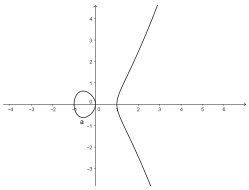
Στην ενότητα αυτή είδαμε μια αλγεβρική μελέτη των αναγώγων αλγεβρικών συνόλων. Η ιδιότητα όμως αυτή είναι εν γένει τοπολογική, και σχετίζεται άμεσα με τη διάσταση του χώρου. Θα δούμε ονομαστικά τα τοπολογικά αντίστοιχα των όσων αναφέραμε ως τώρα. Θυμίζουμε ότι στην αλγεβρική γεωμετρία έχουμε εφοδιάσει τον χώρο μας με την τοπολογία Zariski όπου τα κλειστά ταυτίζονται με τα αλγεβρικά σύνολα.

Ορισμός 1.6. *Ένα υποσύνολο Y ενός τοπολογικού χώρου λέγεται ανάγωγο, εάν δεν υπάρχουν Y_1, Y_2 γνήσια κλειστά υποσύνολα του Y τ.ω $Y = Y_1 \cup Y_2$.*

Παρατήρηση: Αν ένα υποσύνολο Y είναι ανάγωγο, τότε είναι συνεκτικό, όχι όμως το ανάποδο. Γεωμετρικά θα νόμιζε κανείς ότι συνεκτικό είναι ένα ¨εννιαίο' σχήμα, το οποίο όμως μπορεί να οδηγήσει σε παρεξηγήσεις. Παρόλο που μας δίνει μία διαίσθηση του πώς είναι το σχήμα, πρέπει να έχουμε δύο πράγματα καλά στο μυαλό μας: πρώτον ότι η συνεκτικότητα είναι μία τοπολογική έννοια κι εδώ η τοπολογία μας δεν είναι η ευκλείδια αλλά η τοπολογία Zariski και δεύτερον ότι πέρα από το πραγματικό υπάρχει το μιγαδικό επίπεδο. Για να καταλάβουμε τα όσα αναφέραμε ας παρατηρήσουμε τα επόμενα σχήματα.



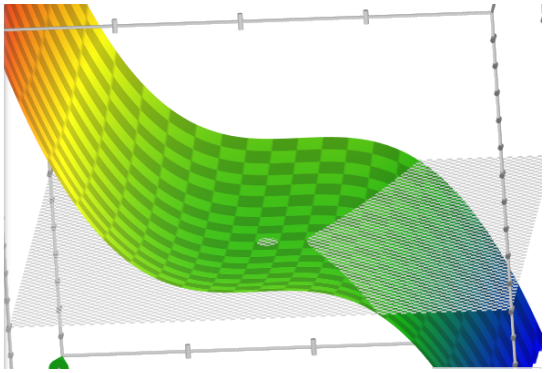
Σχήμα 1.5: Όχι ανάγωγο



Σχήμα 1.6: Ανάγωγο

Το σχήμα 1.5 φαίνεται πως δεν είναι συνεκτικό (τουλάχιστον με την ευκλείδια, πραγματική, διαίσθηση) και όντως εύκολα μπορούμε να δούμε ότι δεν είναι ανάγωγο.
Παρόλαυτα τα φαινόμενα μπορεί να απατούν.

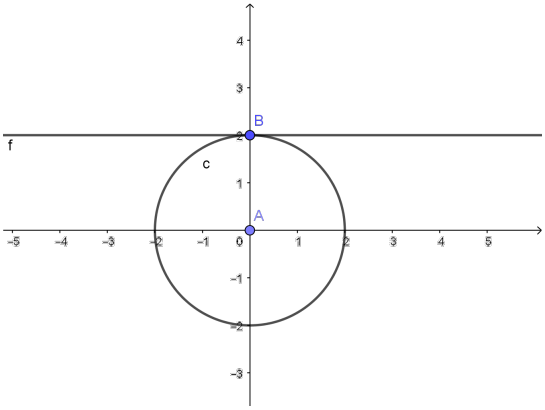
Το σχήμα 1.6 περιγράφεται από το πολυώνυμο $F = Y^2 - X^3 + X$ και εκ πρώτης όψεος φαίνεται μη συνεκτικό. Το λάθος είναι ότι βλέπουμε μόνο τον πραγματικό άξονα. Σε όλο το μιγαδικό επίπεδο, η καμπύλη θα ήταν αυτής της μορφής του σχήματος 1.7



Σχήμα 1.7

Η καμπύλη στο σχήμα 1.6 είναι απλά η τομή του διάφανου επιπέδου που βλέπουμε στο σχήμα 1.7 με την καμπύλη F. Εύκολα δείχνεται ότι το $V(F)$ είναι ανάγωγο.

Το ανάποδο επίσης δεν ισχύει, για παράδειγμα, το σχήμα 1.8 είναι συνεκτικό αλλά όχι ανάγωγο



Σχήμα 1.8

Τα ανάγωγα σύνολα έχουν και κάποιες σημαντικές τοπολογικές ιδιότητες
ΙΔΙΟΤΗΤΕΣ:

1. Αν το Y είναι ανάγωγο, τότε και το $\bar{Y}$ είναι ανάγωγο (το ίδιο ισχύει και για τα συνεκτικά)
2. Αν το Y είναι ανάγωγο, τότε και κάθε μη κενό ανοιχτό υποσύνολο του Y είναι ανάγωγο και πυκνό (Αυτό δεν ισχύει για τα συνεκτικά).
   Συνεπώς, δύο οποιαδήποτε μη κενά σύνολα θα έχουν μεταξύ τους μη κενή τομή. Αυτό μας δίνει να καταλάβουμε ότι τα ανοικτά σύνολα είναι 'μεγάλα' σε μέγεθος.

Εμείς εξετάζαμε στην ενότητα αυτή τα κλειστά ανάγωγα σύνολα. Πράγματι ο παρακάτω ορισμός συμβαδίζει με τα όσα έχουμε δει.

Ορισμός 1.7. *Ένα ανάγωγο κλειστό υποσύνολο του A_k^n λέγεται αφφινική ποικιλότητα, ενώ ένα ανοικτό υποσύνολο μίας αφφινικής ποικιλότητας λέγεται αφφινική ψευδοποικιλότητα (quasi affine variety) .*

Τέλος αξίζει να δούμε την ανάλυση της Noether από μια πιο τοπολογική σκοπιά. Ξεκινάμε με δύο βασικούς ορισμούς.

Ορισμός 1.8. *Ένας τοπολογικός χώρος X λέμε ότι ικανοποιεί DCC (descending chain condition) (κανόνας φθίνουσα ακολουθίας ΚΦΑ) εάν μία οποιαδήποτε φθίνουσα ακολουθία είναι τελικά σταθερή, δηλαδή αν $Z_1 \supseteq Z_2 \supseteq Z_3 \supseteq ...$, τότε $\exists M > 1 : Z_M = Z_{M+1} = ...$ (Ισοδύναμα αν είναι αυστηρά φθίνουσα ακολουθία τότε αυτή μπορεί να είναι μόνο πεπερασμένη και όχι άπειρη)*
Όμοια λέμε ότι ικανοποιεί ACC (ascending chain condition) (κανόνας αύξουσας αλυσίδας ΚΑΑ) εάν οποιαδήποτε αύξουσα ακολουθία είναι τελικά σταθερή.

Προσαρμόζοντας αυτές τις δύο ιδιότητες κατάλληλα μπορούμε να ορίσουμε και να μελετήσουμε την διάσταση χώρων.

Ορισμός 1.9. *Ένας τοπολογικός χώρος X λέγεται Noetherian εάν ικανοποιεί DCC για κλειστά σύνολα.*

Ο αφφινικός χώρος είναι Noetherian . Θυμόμαστε, βέβαια, και την έννοια του Noetherian δακτυλίου πολυωνύμων στην άλγεβρα που είδαμε στην προηγούμενη ενότητα. Αυτές οι δύο έννοιες, όπως θα περίμενε κανεί σχετίζονται.

Γεωμετρία

$k^n = k \times k \times ... \times k +$ **τοπολογία Zariski** $= A_k^n$

Τα επόμενα είναι ισοδύναμα για έναν τοπολογικό χώρο X

1. **Ο X είναι Noetherian (ικανοποιεί DCC (ΚΦΑ) για κλειστά)**
2. **Κάθε μη κενή συλλογή κλειστών υποσυνόλων έχει ελάχιστο στοιχείο**
3. **Αντίστοιχα, κάθε συλλογή ανοιχτών έχει μέγιστο**

Άλγεβρα

$k[X_1, ..., X_n]$

Τα επόμενα είναι ισοδύναμα

1. **Το $k[X_1, ..., X_n]$ ικανοποιεί ACC (ΚΑΑ) για ιδεώδη.**
2. **Κάθε μη κενή συλλογή ιδεωδών στο $k[X_1, ..., X_n]$ έχει μέγιστο στοιχείο. (Αυτή την αντιστοιχία την δίνει το λήμμα του Zorn)**

Το θεώρημα λοιπόν που είδαμε προηγουμένως μεταφράζεται και γενικεύεται στην παρακάτω μορφή

Θεώρημα 1.4. *Αν ο X είναι Noetherian τοπολογικός χώρος, τότε κάθε μη κενό υποσύνολο $Y \subset X$ μπορεί να γραφεί με μοναδικό τρόπο ως $Y = Y_1 \cup Y_2 \cup ... \cup Y_m$, όπου Y_i είναι ανάγωγα κλειστά υποσύνολα και $Y_i \nsubseteq Y_j \forall i \neq j$*

Το πώς συνδέονται όλα αυτά με τις διαστάσεις θα το εξετάσουμε σε παρακάτω ενότητα.

1.4 Hilbert 's Nullstellensatz

Το Nullstellensatz (Θεώρημα σημείων Μηδενισμού) είναι από τα βασικότερα θεωρήματα της άλγεβρας με αμέτρητες εφαρμογές, όχι μόνο στην αλγεβρική γεωμετρία. Χωρίζεται σε ασθενή και ισχυρή μορφή (weak και strong form).
Υποθέτουμε ότι το σώμα μας k είναι αλγεβρικά κλειστό.

Θεώρημα 1.5 (ΑσθενέςNullstellensatz). *Αν I γνήσιο ιδεώδες στο $k[X_1, ..., X_n]$, τότε $V(I) \neq \emptyset$.*

Αν και φαινομενικά απλό στη διατύπωση, η απόδειξη του έχει κάποια λεπτά στοιχεία και δεν μπορεί να αναπτυχθεί χωρίς να μιλήσουμε για βασικές έννοιες όπως επεκτάσεις σωμάτων και $R-$ modules οπότε θα παραλειφθεί. (για απόδειξη δείτε [Har] σελ. 92 ή [Ful89] σελ 21)
Παρατηρείστε ότι αν το σώμα μας δεν είναι αλγεβρικά κλειστό, τότε δεν ισχύει. Για παράδειγμα το $I = (x^2+1) \subset \mathbb{R}[X]$ είναι γνήσιο στο $\mathbb{R}$ αλλά προφανώς $V(I) = \emptyset$

Πριν μιλήσουμε για την ισχυρή μορφή θυμίζουμε ότι $\sqrt{I} = \{f \in k[X_1, ..., X_n] | \exists n \in \mathbb{N} : f^n \in I\}$, το ριζικό ενός ιδεώδους. Προφανώς ισχύει $I \subset \sqrt{I}$. Το I λέγεται ριζικό αν $I = \sqrt{I}$. Από αντιμεταθετική άλγεβρα γνωρίζουμε ότι {ριζικά} $\supset$ {πρώτα} $\supset$ {μέγιστα}, δηλαδή κάθε μέγιστο είναι πρώτο και κάθε πρώτο ιδεώδες είναι ριζικό.

Θεώρημα 1.6 (**HILBERT 'S NULLSTELLENSATZ**). *Έστω I ιδεώδες στο $k[X_1, ..., X_n]$ (k αλγεβικά κλειστό). Τότε $I(V(I)) = \sqrt{I}$*

(Για μια πιο γενική μορφή δείτε [Mum70] σελ.131) Παρατήρηση: Με άλλα λόγια το θεώρημα λέει το εξής: Αν $F_1, ..., F_r, G \in k[X_1, ..., X_n]$ και το G μηδενίζει όπου μηδενίζουν και τα $F_1, ..., F_r$, (δηλαδή $G \in I(V(F_1, .., F_r)))$, τότε ισχύει ότι $G^N = A_1F_1 + ... + A_rF_r$, για κάποιο $N > 0$ και $A_i \in k[X_1, ..., X_n]$ (δηλαδή $G \in \sqrt{(F_1, ..., F_r)})$.

Θεωρώντας γνωστή την ασθενή μορφή του θεωρήματος, μπορούμε να αποδείξουμε σχετικά πιο εύκολα την ισχυρή.

Απόδειξη. Αρχικά θα δείξουμε την εύκολη κατεύθυνση, ότι δηλαδή $\sqrt{I} \subset I(V(I))$.
Πράγματι, αφού $I \subset \sqrt{I} \Rightarrow V(\sqrt{I}) \subset V(I)$. Θα δείξουμε την αντίστροφη σχέση. Έστω $P \in V(I) \Rightarrow F(P) = 0 \quad \forall F \in I$. Έστω $G \in \sqrt{I} \Rightarrow G^n \in I$ για κάποιο $n \in N \Rightarrow G^n(P) = 0 \Rightarrow G(P) = 0 \quad \forall G \in I \Rightarrow P \in V(\sqrt{I})$.
Συνεπώς $V(I) = V(\sqrt{I})$
Όμως από πρόταση 3 έχουμε $\sqrt{I} \subset I(V(\sqrt{I})) = I(V(I))$ και παίρνουμε την επιθυμητή σχέση.
Η δυσκολία έγκειται στον αντίθετο εγκλεισμό. Έστω $G \in I(V(F_1, ..., F_r)), F_i \in k[X_1, ..., X_n]$. Έστω $J = (F_1, ..., F_r, X_{n+1}G - 1) \subset k[X_1, ..., X_n, X_{n+1}]$. Τότε $V(J) \subset A_k^{n+1}$. Παρατηρούμε ότι $V(J) = \emptyset$. Πράγματι, εάν $P \in V(J)$, τότε $F_i(P) = 0 \forall i$. Όμως από την υπόθεση το G μηδενίζει όπου και τα F_i, συνεπώς $G(P) = 0 \Rightarrow (X_{n+1}G - 1)(P) \neq 0$.
Από την ασθενή μορφή, αφού $V(J) = \emptyset$, έχουμε ότι $1 \in J$ και δηλαδή υπάρχει εξίσωση

$$1 = \sum_i A_iF_i + B(X_{n+1}G - 1), A, B \in k[X_1, ..., X_n, X_{n+1}].$$

Θέτουμε $Y = 1/X_{n+1}$, βρίσκουμε τον μέγιστο βαθμό του όρου X_{n+1} στην παραπάνω εξίσωση και πολλαπλασιάζουμε την εξίσωση με αρκετά μεγάλη δύναμη του Y ώστε να προκύψει μία εξίσωση της μορφής $Y^N = \sum C_i F_i + D(G - Y) \in k[X_1, ..., X_n, Y], C_i, D \in k[X_1, ..., X_n, Y]$. Αντικαθιστώντας το G με το Y παίρνουμε το επιθυμητό αποτέλεσμα.

□

Η απόδειξη αυτή είναι χάρη στον Rabinowitch .

Από το Nullstellensatz προκύπτουν άμεσα κάποια πολύ βασικά λήμματα που στην ουσία είναι ο κορμός των όσων θα μελετήσουμε παρακάτω.

Πρόταση 1.14. *Αν I ριζικό ιδεώδες στο $k[X_1, ..., X_n]$ τότε $I(V(I)) = I$. Συνεπώς υπάρχει 1-1 αντιστοιχία μεταξύ ριζικών ιδεωδών και αλγεβρικών συνόλων.*

Πρόταση 1.15. *Αν I πρώτο ιδεώδες, τότε $V(I)$ είναι ανάγωγο. Υπάρχει 1-1 αντιστοιχία μεταξύ πρώτων ιδεωδών και αλγεβρικών συνόλων. Τα μέγιστα ιδεώδη αντιστοιχούν σε σημεία.*

Πρόταση 1.16. *Έστω $F \in k[X_1, ..., X_n], F = F_1^{n_1} \cdot .... \cdot F_r^{n_r}$ η ανάλυση του F σε ανάγωγους παράγοντες. Τότε $V(F) = V(F_1) \cup ... \cup V(F_r)$ είναι η ανάλυση του $V(F)$ σε ανάγωγους παράγοντες και $I(V(F)) = (F_1 \cdot ... \cdot F_r)$. Υπάρχει 1-1 αντιστοιχία μεταξύ των αναγώγων πολυωνύμων $F \in k[X_1, ..., X_n]$ (ταυτίζοντας το F με το $\lambda F, \lambda \in k, \lambda \neq 0$) και των αναγώγων υπερεπιφανειών στο $A^n(k)$*

Πρόταση 1.17. *Έστω I ιδεώδες του $k[X_1, ..., X_n]$. Τότε το $V(I)$ είναι πεπερασμένο σύνολο αν-ν $\dim_k(k[X_1, ..., X_n]/I) < \infty$. Αν αυτό προκύπτει τότε το σύνολο των σημείων του $V(I)$ είναι λιγότερα ή ίσα του $dim_k(k[X_1, ..., X_n]/I)$. , δηλαδή $|V(I)| \leq \dim_k(k[X_1, ..., X_n]/I)$*

Η πρόταση 1.7 στην ουσία είναι το Nullstellensatz διαφορτικά διατυπωμένο. Την 1-1 αντιστοιχία πρώτων ιδεωδών και αναγώγων πολυωνύμων την έχουμε ήδη δει από την πρόταση 1.11, ενώ για τα μέγιστα από την πρόταση 1.10.
Θυμίζουμε καταρχάς τη βασική σχέση που πρέπει συνέχεια να έχετε κατά νου:
{ριζικά ιδεώδη} $\supset$ {πρώτα ιδεώδη}$\supset$ {μέγιστα ιδεώδη}, δηλαδή κάθε μέγιστο ιδεώδες είναι πρώτο και κάθε πρώτο είναι ριζικό.
Αν με j συμβολίζουμε τα ριζικά ιδεώδη, p τα πρώτα και m τα μέγιστα, τότε μπορούμε πάντα να βρούμε μία σχέση εγκλεισμού $j \subset p \subset m$. Παίρνοντας τα σημεία μηδενισμού αντιστρέφονται οι εγκλεισμοί και θα έχουμε $V(m) \subset V(p) \subset V(j)$. Δηλαδή τα μέγιστα ιδεώδη στην άλγεβρα αντιστοιχούν στα μικρότερα δυνατά υποσύνολα στον αφφινικό χώρο. Η πρόταση 1.15 μας επιβεβαιώνει ότι αυτά τα μικρότερα δυνατά υποσύνολα δεν είναι τίποτα άλλο παρά σημεία.

Μπορούμε έτσι να σχηματίσουμε ένα υποτυπόδες διάγραμμα που να εξηγεί αυτή την αντιστοιχία.

Γεωμετρία		**Άλγεβρα**
$A_k^n = k^n +$ τοπολογία Zariski		$k[X_1, ..., X_n]$
{χλειστά/αλγεβρικά υποσύνολα}	$\longleftrightarrow$	{ριζικά ιδεώδη}.
{ Αφφινικές ποικιλότητες }	$\longleftrightarrow$	{πρώτα ιδεώδη}= {Spec$(k[X_1, ..., X_n])$}
A_k^n={ σημεία στον A_k^n} $\ni (a_1, ..., a_n)$	$\longleftrightarrow$	{μέγιστα ιδεώδη } $= MaxSpec(k[X_1, ..., X_n]) \ni m = (X_1 - a_1, ..., X_n - a_n)$

Η πρόταση 1.16 είναι επίσης προφανής, αρκεί να σκεφτεί κανείς ότι $\sqrt{F_1^{n_1}...F_r^{n_r}} = \sqrt{F_1...F_r} = F_1...F_r$.

Η μόνη πρόταση που χρίζει αιτιολόγησης, και η οποία ίσως είναι και η πιο σημαντική είναι η πρόταση 1.17. Για να την αποδείξουμε, χρειαζόμαστε πρώτα ένα χρήσιμο λήμμα από την Άλγεβρα:

Λήμμα 1.1. *α Έστω V ένα αλγεβρικό σύνολο στο $A_k^n, P \in A_k^n$ σημείο τ.ω $P \notin V$. Τότε υπάρχει πολυώνυμο $F \in k[X_1, ..., X_n] : F(Q) = 0 \quad \forall Q \in V$ και $F(P) = 1$.*

β Έστω $\{P_1, ..., P_r\}$ πεπερασμένη συλλογή διακεκριμένων σημείων στο A_k^n . Τότε υπάρχουν πολυώνυμα $F_1, ..., F_r$ τέτοια ώστε $F_i(P_j) = 0 \forall i \neq j, F_i(P_i) = 1$

Απόδειξη. α Παρατηρούμε ότι $V \subsetneq V \cup \{P\}$. Θα δείξουμε ότι $I(V) \neq I(V \cup \{P\})$.
Έστω ότι $I(V) = V \cup \{P\} \Rightarrow V(I(V)) = V(I(V \cup \{P\})) \Rightarrow V = V(I(V \cup \{P\}))$. (Παρατηρείστε ότι γνωρίζουμε ότι V αλγεβρικό συνεπώς $V(I(V)) = V$).
Όμως $V \subsetneq V \cup \{P\} \subset V(I(V \cup \{P\}))$ καταλήγοντας σε άτοπο. Συνεπώς $I(V) \neq I(V \cup \{P\})$.
Μάλιστα $V \subsetneq V \cup \{P\} \Rightarrow I(V \cup \{P\}) \subsetneq I(V)$. Συνεπώς $\exists F \in I(V) : F \notin I(V \cup \{P\}) \Rightarrow F(Q) = 0 \quad \forall Q \in V, F(P) \neq 0$. Θεωρώ $G = \frac{F}{F(P)}$ κι έχω το ζητούμενο.

β Απλή εφαρμογή του (α), θέτοντας $V = \{P_1, ..., P_n\} - \{P_i\}$ και παρατηρώντας ότι είναι αλγεβρικό ως πεπερασμένη ένωση αλγεβρικών.

□

Μπορούμε τώρα να αποδείξουμε την Πρόταση 1.17

Απόδειξη. Έστω $dim_k(k[X_1, ..., X_n]/I) < \infty$ και $P_1, ..., P_r \in V(I)$. Διαλέγουμε πολυώνυμα $F_1, ..., F_r \in k[X_1, ..., X_n]$ τ.ω $F_i(P_j) = 0 \quad \forall i \neq j, F_i(P_i) = 0$ (Λήμμα 1). Έστω $R = k[X_1, ..., X_n]/I$ ο δακτύλιος πηλίκο. Αν $f_i = F_i + R$, τότε θα δείξουμε ότι τα f_i είναι γραμμικά ανεξάρτητα στο R πάνω από το k. (Προφανώς $F_i \notin I \Rightarrow f_i \neq 0$) Έστω $\sum_{i=1}^r \lambda_i f_i = 0, \lambda_i \in k \Rightarrow \sum_{i=1}^r \lambda_i F_i \in I$. Συνεπώς $(\lambda_1 F_1 + ...\lambda_r F_r)(P_i) = 0 \forall i = 1, ..., r \Rightarrow \lambda_i = 0 \forall i = 1, ..., r$. Συνεπώς f_i γραμμικά ανεξάρτητα πάνω από το k και άρα $r \leq dim_k(k[X_1, ..., X_n]/I)$.
Ανάποδα, έστω $V(I) = \{P_1, ..., P_r\}$ πεπερασμένο και έστω $P_i = (a_{i1}, ..., a_{in})$. Θεωρούμε $F_j = \prod_{i=1}^r (X_j - a_{ij}), j = 1, ..., r$. Τότε $F_j(P_i) = 0 \quad \forall i = 1, .., r \Rightarrow F_j \in I(V(I)) = \sqrt{I} \Rightarrow \exists N_j > 0 : F_j^{N_j} \in I$. Διαλέγουμε $N > max\{N_j, j = 1, ..., r\}$. Προφανώς $F_j^N \in I$ για κάθε $j = 1, .., r$. Θεωρούμε $f_j = F_j + R$ και $x_j = X_j + R$. Τότε $f_j^N = 0$ Αναπτύσσοντας το $F_j^N = \prod_{i=1}^r (X_j - a_{ij})^N$ και παίρνωντας την εικόνα του του στο R βλέπουμε ότι το x_j^{rN} γράφεται ως γραμμικός συνδιασμός των $1, x_j, ..., x_j^{rN-1}$. Έστω $x_j^{rN} = \sum_{i=0}^{rN-1} \lambda_i x_j^i$ (1) Τότε πολλαπλασιάζοντας με x_j παίρνουμε ότι $x_j^{rN+1} = \sum_{i=0}^{rN-1} \lambda_i x_j^{i+1}$. Αντικαθιστώντας το x_j^{Rn} που θα προκύψει από τη σχέση (1), βλέπουμε ότι το x_j^{rn+1} γράφεται ως k- γραμμικός συνδιασμός των $1, x_j, ..., x_j^{rN-1}$. Συνεχίζοντας επαγωγικά βλέπουμε κατευθείαν ότι το x_j^s μπορεί να γραφεί ως k -γραμμικός συνδιασμός των $1, x_j, ..., x_j^{rN-1}$ για κάθε $s >= 0$. Κάνοντας την ίδια διαδικασία και για τα υπόλοιπα j συμπεραίνουμε ότι το σύνολο $\{x_1^{m_1} \cdot .... \cdot x_n^{m_n}, m_i < rN\}$ παράγει όλο το R ως διανυσματικό χώρο πάνω από το k. Συνεπώς ο R είναι πεπερασμένης διάστασης. □

Πρωτού προχωρήσουμε παρακάτω είναι χρήσιμο να μελετήσουμε πώς εφαρμόζονται όλα αυτά που μάθαμε, στο επίπεδο, δηλαδή στο A_k^2.

1.5 Αλγεβρικά σύνολα στο Επίπεδο

Λόγω της μικρής του διάστασης, το επίπεδο έχει κάποιες χαρακτηριστικές ιδιότητες που δεν γενικεύονται στις μεγαλύτερες διαστάσεις. Παρόλαυτα, παραμένουν αρκετά σημαντικές για την ανάπτυξη της θεωρίας όπως θα δούμε παρακάτω.

Στόχος μας είναι να περιγράψουμε πλήρως τα αλγεβρικά σύνολα στο επίπεδο (Θυμίζω έχουμε ήδη δει όλα τα αλγεβρικά σύνολο στο A_k^1 από την πρόταση 1.4). Ξεκινάμε με μία βασική πρόταση.

Πρόταση 1.18. *Έστω $F, G \in k[X,Y]$ πολυώνυμα χωρίς κοινούς παράγοντες (δηλαδή δεν υπάρχει κάποιο μη σταθερό πολυώνυμο H που να τα διαιρεί και τα δύο). Τότε το $V(F,G) = V(F) \cap V(G)$ αποτελείται από πεπερασμένα σημεία.*

Απόδειξη. Έστω F, G πολυώνυμα χωρίς κοινούς παράγοντες στο $k[X,Y] = k[X][Y]$. Τότε δεν θα έχουνε κοινούς παράγοντες ούτε στο $k(X)[Y]$, όπου $k(X)$ το σώμα κλασμάτων του $k[X]$. (Θυμίζουμε από την άλγεβρα ότι σώμα κλασμάτων ενός δακτυλίου R είναι το μικρότερο σώμα που περιέχει το R. Τα στοιχεία του $k(X)$ είναι της μορφής $z = \frac{f}{g}, f, g \in k[X], g \neq 0$.) Αφού $k(X)$ σώμα, άρα $k(X)[Y]$ ΠΚΙ (Γενικά ισχύει ότι αν R σώμα τότε $R[X]$ ΠΚΙ). Όμως, $(F,G) = 1$ στο $K(X)[Y]$ αφού δεν έχουν κοινούς παράγοντες και άρα $\exists R, S \in k(X)[Y]$: $RF + SG = 1$. Αφού $R = a_nY^n + ... + a_1Y + a_0, a_i \in k(X) \Rightarrow a_i = H_i/T_i \in k[X]$, πολλαπλασιάζοντας με $D_1 = T_0 \cdot ... \cdot T_n$ έχουμε ότι $DR = A_1 \in k[X,Y], D_1 \in k[X]$. Όμοια υπάρχει $D_2 \in k[X] : D_2S = B_1 \in k[X,Y]$. Θέτοντας $D = D_1D_2$ έχουμε ότι $D \in k[X,Y]$ και $DR = A \in k[X,Y], RS = B \in k[X,Y]$.
Συνεπώς $AF + BG = DRF + DSG = D$. Αν $(a,b) \in V(F,G)$, τότε $D(a) = 0$. Όμως $D \in k[X]$ και άρα έχει πεπερασμένο αριθμό σημείων μηδενισμού. Συμπεραίνουμε, λοιπόν, ότι υπάρχει πεπερασμένος αριθμός στοιχείων στη X συντεταγμένη στο $V(F,G)$. Κάνοντας την ίδια διαδικασία και για την Υ- συντεταγμένη, προκύπτει το ζητούμενο. □

Αυτό προφανώς δεν ισχύει για μεγαλύτερες διαστάσεις. Για παράδειγμα, η σφαίρα που δίνεται από την εξίσωση $F = X^2 + Y^2 + Z^1 - 1$ με το οριζόντιο επίπεδο $G = Z$ τέμνονται σε άπειρα σημεία (τον ησιμερινό).

Θυμίζουμε ότι τα ανάγωγα αλγεβρικά σύνολα αντιστοιχούν σε πρώτα ιδεώδη. Η παρακάτω πρόταση εξετάζει τη μορφή αυτών των πρώτων ιδεωδών στις 2 διαστάσεις.

Πρόταση 1.19. *Αν F ανάγωγο πολυώνυμο στο $k[X,Y]$ και $V(F)$ άπειρο, τότε $I(V(F)) = (F)$ και $V(F)$ ανάγωγο*

Απόδειξη. Η απόδειξη είναι άμεση. Αν $G \in I(V(F))$ τότε αρκεί να δείξω ότι $G \in (F)$. Όμως το G μηδενίζει τουλάχιστον όπου μηδενίζει και το F, άρα $V(F,G)$ άπειρο. Από την προηγούμενη πρόταση συμπεραίνουμε ότι F και G έχουν κοινούς παράγοντες. Επειδή όμως F ανάγωγο, συνεπώς το F διαιρεί το G και άρα $G \in (F)$. Συνεπώς $I(V(F)) = V(F)$. Γνωρίζουμε από την άλγεβρα ότι το (F) είναι πρώτο ιδεώδες αφού F ανάγωγο, άρα $V(F)$ ανάγωγο. □

Είμαστε σε θέση πια να χαρακτηρίσουμε πλήρως τα ανάγωγα αλγεβρικά υποσύνολα του A_k^2.

Θεώρημα 1.7. *Έστω k άπειρο. Τότε τα ανάγωγα αλγεβρικά υποσύνολα του A_k^2 είναι τα :*

α A_k^2

β $\emptyset$

γ Σημεία

δ Ανάγωγες επίπεδες καμπύλες $V(F)$, όπου F ανάγωγο πολυώνυμο και $V(F)$ άπειρο.

Απόδειξη. Έστω V ανάγωγο αλγεβρικό υποσύνολο του A_k^2. Τότε $V = V(S)$, $S \subset k[X,Y]$. Αν $V = A_k^2 = V(0)$ τότε είναι ανάγωγο γιατί (0) πρώτο ιδεώδες αφού $k[X,Y]$ ακεραία περιοχή. Αν $V = \emptyset = V(A_k^2)$ τετριμμένα ανάγωγο. Αν $V = \{P\} = \{(a,b)\} \Rightarrow I(V) = (X-a, Y-b)$ μέγιστο και άρα πρώτο ιδεώδες, συνεπώς V ανάγωγο. Αν $V = \{P_1, ..., P_s\} = \{P_1\} \cup ... \cup \{P_s\}$ αλγεβρικό ως πεπερασμένη ένωση αλγεβρικών

αλλά προφανώς όχι ανάγωγο.
Έστω V άπειρο και $F \in I(V)$, όπου $I(V)$ πρώτο και F μη σταθερό πολυώνυμο. Αν F όχι ανάγωγο τότε υπάρχει κάποιος ανάγωγος παράγοντας του F που να ανήκει στο $I(V)$, αφού $I(V)$ πρώτο ιδεώδες. Έστω λοιπόν H ανάγωγο πολυώνυμο στο $k[X,Y]$ τ.ω $H \in I(V)$. Τότε προφανώς $(H) \subset I(V)$. Αν $G \in I(V)$ και $G \notin (H)$, τότε $V \subset V(F,G)$ πεπερασμένο που είναι άτοπο. Άρα $I(V) = (H)$ και άρα πρώτο ιδεώδες. $\square$

Κεφάλαιο 2

Αφφινικές ποικιλότητες

Στην προηγούμενη ενότητα μελετήσαμε τις βασικές έννοιες της αλγεβρικής γεωμετρίας. Για να προχωρήσουμε παρακάτω όμως, χρειάζεται πρώτα να αναπτύξουμε βασικά εργαλεία.
Από εδώ και στο εξής θα θεωρούμε πάντα το σώμα μας αλγεβρικά κλειστό. Θα δουλεύουμε στον αφφινικό χώρο A_k^n. Θα αναφερόμαστε στις αφφινικές ποικιλότητες απλά ως ποικιλότητες .
Όλοι οι δακτύλιοι και τα σώματα θα περιέχουν το k ως υποδακτύλιο. Ως ομομορφισμό $\phi : R \to S$ τέτοιων δακτυλίων, θα εννοούμε έναν ομομορφισμό δακτυλίων τ.ω $\phi(\lambda) = \lambda \quad \forall \lambda \in k$.
Όντας απλά μία εισαγωγή, δεν θα επικεντρωθούμε τόσο στις αποδείξεις, καθώς είναι περισσότερο τεχνικές και αφορούν κυρίως το κομμάτι της αντιμεταθετικής άλγεβρας.

2.1 Δακτύλιοι Συντεταγμένων και Πολυωνυμικές Απεικονίσεις

Έστω $V \subset A^n$ μία ποικιλότητα. Τότε το $I(V)$ είναι πρώτο ιδεώδες στο $k[X_1, ..., X_n]$ και συνεπώς το $k[X_1, ..., X_n]/I$ είναι ακεραία περιοχή. Θα το συμβολίζουμε με $\Gamma(V) = k[X_1, ..., X_n]/I(V)$ και θα το λέμε δακύλιο συντεταγμένων του V . Ο λόγος που ονομάζεται έτσι θα εξηγηθεί παρακάτω.
Για οποιοδήποτε μη κενό σύνολο V, συμβολίζουμε με $\zeta(V, k)$ το σύνολο όλων των συναρτήσεων από το V στο k. Το $\zeta(V, k)$ μπορούμε να το φτιάξουμε σε δακτύλιο με τον συνήθη τρόπο: Αν $f, g \in \zeta(V, k), (f + g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x), \forall x \in V$. Συνήθως ταυτίζουμε το k με τον υποδακτύλιο του $\zeta(V, k)$ που αποτελείται από όλες τις σταθερές συναρτήσεις.
Οι συναρτήσεις βέβαια που μας ενδιαφέρουν εδώ είναι οι πολυωνυμικές. Συγκεκριμένα, δοσμένης μίας ποικιλότητας $V \subset A^n$ ονομάζουμε μία συνάρτηση $f \in \zeta(V, k)$ πολυωνυμική , εάν υπάρχει πολυώνυμο $F \in k[X_1, ..., X_n]$ τ.ω $f(a_1, ..., a_n) = F(a_1, ..., a_n)$ για κάθε $(a_1, .., a_n) \in V$. Οι πολυωνυμικές συναρτήσεις συνιστούν έναν υποδακτύλιο του $\zeta(V, k)$ που περιέχει το k. Πράγματι δεν είναι δύσκολο να ελέγξουμε ότι το σύνολο των πολυωνυμικών συναρτήσεων είναι ομάδα με πράξη την πρόσθεση και ισχύει προφανώς η προσεταιριστικότητα και επιμεριστηκότητα. Το ουδέτερο στοιχείο προφανώς είναι η μοναδιαία συνάρτηση $f(a_1, ..., a_n) = 1 \quad \forall (a_1, .., a_n) \in V$ και ισχύει η αντιμεταθετικότητα. Όλες αυτές οι ιδιότητες είναι προφανείς αν ταυτίσουμε στο μυαλό μας τις πολυωνυμικές συναρτήσεις με πολυώνυμα. Δύο πολυώνυμα F, G ορίζουν την ίδια πολυωνυμική συνάρτηση αν $(F - G)(a_1, ..., a_n) = 0 \quad \forall (a_1, ..., a_n) \in V$, δηλαδή αν-ν $F - G \in I(V)$. Μπορούμε λοιπόν να ταυτίσουμε το $\Gamma(V)$ με τον υποδακτύλιο του $\zeta(V, k)$ που αποτελείται από όλες τις πολυωνυμικές συναρτήσεις. Συνεπώς έχουμε δύο εξίσου σημαντικούς τρόπους να σκεφτόμαστε ένα στοιχείο του $\Gamma(V)$: ως συνάρτηση στο V ή ως κλάση ισοδυναμίας πολυωνύμων.
Το πρώτο κομμάτι ίσως χρειάζεται περισσότερη εξήγηση, δεδομένου ότι από εκεί προκύπτει και το όνομα δακτύλιος συντεταγμένων. Ένα πιο οικείο ίσως παράδειγμα είναι στη διαφορική γεωμετρία. Στη διαφορική γεωμετρία αντί για ποικιλότητες χρησιμοποιούμε πολλαπλότητες. Το κύριο χαρακτηριστικό των πολλαπλοτήτων είναι ότι καλύπτονται από συλλογή χαρτών, ή αλλιώς τοπικά συστήματα συντεταγμένων (U_i, ϕ_i) όπου

U_i ανοικτό σύνολο και $\phi_i : U_i \to \mathbb{R}^n$, όπου κάθε στοιχείο $p \in U$ απεικονίζεται στο $\phi(p) = (x_1, ..., x_n)$. Τα $(x_1, ..., x_n)$ λέγονται συντεταγμένες του p.
Η κατάσταση εδώ είναι αρκετά παρόμοια. Ο αντίστοιχος $\mathbb{R}^n$ χώρος για εμάς είναι ο αφφινικός χώρος A^n_k στον οποίο έχουμε συντεταγμένες υπό τη μορφή πάλι μιας n-άδας στοιχείων $(a_1, ..., a_n)$. Δείξαμε όμως από πάνω ότι κάθε στοιχείο του $\Gamma(V)$ αντιστοιχεί σε μία πολυωνυμική απεικόνιση από το V στο k δηλαδή μία ¨καλή' συνάρτηση που απεικονίζει κάθε συντεταγμένη του V σε ένα στοιχείο του k. Εξού λοιπόν και η ονομασία δακτύλιος συντεταγμένων.

Πέρα από τη ποικιλότητα V συχνά μας ενδιαφέρουν και τα υποσύνολά της. Όπως θα περίμενε κανείς, ένα υποσύνολο $W \subset V \subset A^n$ λέγεται υποποικιλότητα του V εάν είναι το ίδιο ποικιλότητα.
Η μετάβαση από το $k[X_1, ..., X_n]$ στο $k[X_1, ..., X_n]/I$ μεταφέρει όπως θα δούμε αρκετές ιδιότητες. Θα διατυπώσουμε την επόμενη πρόταση στη γενική της μορφή και μετά θα την προσαρμόσουμε στο κομμάτι που μας ενδιαφέρει.

Πρόταση 2.1. *Έστω I ιδεώδες σε έναν δακτύλιο R, π: $R \to R/I$ ο φυσικός ομομορφισμός.*

α *Κάθε ιδεώδες J' του R/I, το $\pi^{-1}(J') = J$ είναι ιδεώδες του R που περιέχει το I, και για κάθε ιδεώδες J που περίεχει το I, το $\pi(J) = J'$ είναι ιδεώδες στο R/I. Συνεπώς υπάρχει μία φυσική 1-1 αντιστοίχιση μεταξύ {ιδεωδών του R/I } και {ιδεωδών του R που περιέχουν το I}.*

β *Το J' είναι ριζικό (αντ. πρώτο, αντ. μέγιστο) αν-ν το J είναι ριζικό (αντ. πρώτο, αντ. μέγιστο).*

γ *Αν J' είναι πεπερασμένα παραγόμενο τότε και το J είναι πεπερασμένα παραγόμενο. Συνεπώς ο R/I είναι Noetherian αν ο R είναι Noetherian . Οποιοσδήποτε λοιπόν δακτύλιος $k[X_1, ..., X_n]/I$ είναι Noetherian .*

Απόδειξη. α Έστω J' ιδεώδες του R/I και π:$R \to R/I$, $\pi^{-1}(J') = J = \{y \in R : \pi(y) \in J'\}$
Αφού J' ιδεώδες άρα $0_{R/I} \in J' \Rightarrow I \subset \pi^{-1}(J') = J$, αφού $\pi(I) = 0 \in J'$.
Έστω $x \in J, y \in R$. Τότε $\pi(xy) \overset{\text{ομομ.}}{=} \pi(x)\pi(y) \in J'$ αφού $\pi(x) \in J'$ και J' ιδεώδες. Όμοια αν $x, y \in J$ τότε $\phi(x - y) \overset{\text{ομομ.}}{=} \phi(x) - \phi(y) \in J'$ αφού $(J', +)$ ομάδα. Άρα $(J, +)$ ομάδα, άρα J ιδεώδες.
Αντίστροφα, έστω $I \subset J$ ιδεώδες του R. Θέλουμε να δείξουμε ότι $\pi(J) = J'$ ιδεώδες.
Έστω $x + I \in J', y + I \in R/I$, τότε $(x + I)(y + I) = xy + I \in \pi(J)$, αφού J ιδεώδες και $x \in J \Rightarrow xy \in J \Rightarrow xy + I \in \pi(J)$. Εύκολα βλέπουμε επίσης ότι $(J', +)$ ομάδα, άρα J' ιδεώδες

β Έστω J' ριζικό και $J = \pi^{-1}(J')$. Έστω $x^n \in J, x \in R, n \in \mathbb{N} \Rightarrow x^n + i \in J' \overset{J'\text{ριζικό}}{\Rightarrow} x + I \in J' \Rightarrow x \in J$ και άρα J ριζικό.

Έστω J ριζικό και $J' = \pi(J)$
Έστω $x^n + I \in J' \Rightarrow x^n \in J \overset{J\text{ριζικό}}{\Rightarrow} x \in J \Rightarrow x + I \in J'$ και άρα J' ριζικό.
Ακριβώς όμοια δουλεύουμε για τα πρώτα και μέγιστα ιδεώδη.

γ Έστω $J = (x_1, ..., x_r)$. Τότε $J' = (x_1 + I, ..., x_r + I)$ (γιατί;)και άρα πεπερασμένα παραγόμενο. Αφού υπάρχει 1-1 αντιστοίχιση μεταξύ των ιδεωδών του R που περιέχουν το I και των ιδεωδών του R/I συμπεραίνουμε ότι αν ο R είναι Noetherian , τότε για κάθε J' ιδεώδες του R/I , το $J = \pi^{-1}(J)$ είναι ιδεώδες του R και άρα πεπερασμένα παραγόμενο. Συνεπώς το $\pi(J) = J'$ πεπερασμένα παραγόμενο. Άρα R/I είναι Noetherian . Άρα αφού $k[X_1, ..., X_n]$ είναι Noetherian (Θεώρημα βάσης του Hilbert)συμπεραίνουμε ότι και $k[X_1, ..., X_n]/I$ είναι Noetherian .

□

Μεταφράζοντας αυτή την πρόταση στην αλγεβρική γεωμετρία, βλέπουμε ότι υπάρχει 1-1 αντιστοίχιση μεταξύ των αλγεβρικών συνόλων του V και των ριζικών ιδεωδών του $\Gamma(V)$, καθώς επίσης ότι τα ανάγωγα αλγεβρικά σύνολα αντιστοιχούν (αντ. σημεία) αντιστοιχούν σε πρώτα ιδεώδη (αντ. μέγιστα ιδεώδη).
Συνεπώς εύκολα καταλήγουμε στο συμπέρασμα ότι υπάρχει 1-1 αντιστοίχιση μεταξύ των αλγεβρικών υποσυνόλων (αντ, υποποικιλότητες , αντ. σημείων) του V με τα ριζικά ιδεώδη (αντ. πρώτα ιδεώδη, αντ. μέγιστα ιδεώδη) του $\Gamma(V)$. Η απόδειξη είναι άμεση από τα παραπάνω.

Εάν το V είναι μεμονωμένο σημείο, $V = \{P\}, P = (a_1, ..., a_n) \in A^n_k$ τότε $I(V) = (X_1 - a_1, ..., X_n - a_n)$ μέγιστο ιδεώδες. Συνεπώς $\Gamma(V) = k[X_1, ..., X_n]/I(V) = k$. Πράγματι από την πρόταση 1.9 έχουμε ότι αν $f \in \Gamma \Rightarrow f = F+I(V), F \in k[X_1, ..., X_n]$ και το F μπορεί να γραφεί ως $F = \sum_{i=0} r_i(X_1-a_1)^{i_1}\cdot...\cdot(X_n-a_n)^{i_n}$, $r_i \in k$. Θεωρώντα $i = 0$ την περίπτωση όπου $i_1, ..., i_n = 0$ και παίρνοντας $modI(V)$ έχουμε ότι $f = r_0 + I(V)$. Επιπλέον $k \subset \Gamma(V)$ και άρα $\Gamma(V) \cong k$.
Υπάρχει όμως και πιο εύκολος, λιγότερο αλγεβρικός τρόπος να καταλήξουμε σε αυτό το συμπέρασμα. Εάν σκεφτούμε το $\Gamma(V)$ ως τις πολυωνυμικές απεικονίσεις από το V στο k, έχουμε ότι $\Gamma(V) = \{f : V \to k, f \quad \text{πολυωνυμική}\} = \{f : \{P\} \to k, f \quad \text{πολυωνυμική}\} = \{f_x : P \mapsto x, x \in k\} \cong \{k\}$.

Πολυωνυμικές απεικονίσεις Εάν ταυτίσουμε το k με το A^1 τότε οι πολυωνυμικές συναρτήσεις είναι απεικονίσεις από το V στο A^1. Μπορούμε να γενικεύσουμε αυτή την έννοια.

Ορισμός 2.1. *Έστω $V \subset A^n, W \subset A^m$ ποικιλότητες. Μία συνάρτηση $\phi : V \to W$ λέγεται πολυωνυμική απεικόνιση εάν υπάρχουν πολυώνυμα $T_1, ..., T_m \in k[X_1, ..., X_n]$ τ.ω $\phi(a_1, ..., a_n) = (T_1(a_1, ..., a_n), ..., T_m(a_1, ..., a_n) = (T_1, ..., T_m)(a_1, ..., a_m)$ για κάθε $(a_1, ..., a_n) \in V$.*

Όπως και στις πολλαπλότητες όπου μελετάμε τις λείες απεικονίσεις $f : M \to N$ μέσω των χαρτών τους/τοπικού συστήματος συντεταγμένων, έτσι κι εδώ συχνά μας βολεύει να μελετάμει τις πολυωνυμικές απεικονίσεις μέσα από τους δακτυλίους συντεταγμένων.
Γενικά, κάθε συνάρτηση $\phi : V \to W$ επάγει έναν ομομορφισμό $\tilde{\phi} : \zeta(W, k) \to \zeta(V, k)$,όπου $\tilde{\phi}(f) = f \circ \phi$. Πράγματι δεν είναι δύσκολο να δούμε ότι ο $\tilde{\phi}$ είναι ομομορφισμός. Μάλιστα, εάν ϕ πολυωνυμική απεικόνιση, τότε $\tilde{\phi}(\Gamma(W)) \subset \Gamma(V)$, και συνεπώς ο $\tilde{\phi}$ περιορίζεται σε ομομορφισμό, που θα τον συμβολίζουμε επίσης με $\tilde{\phi}$ από το $\Gamma(W)$ στο $\Gamma(V)$. Πράγματι, εάν $f = F + I(W) \in \Gamma(W), F \in k[X_1, ..., X_m]$, τότε $\tilde{\phi}(f) = f \circ \phi = F(T_1, ..., T_m) + I(V) \in \Gamma(V), T_i \in k[X_1, ..., X_n]$. Αυτό μοιάζει πολύ με τις δυϊκές απεικονίσεις που βλέπουμε πάλι στη διαφορική γεωμετρία, όπου εάν V, W δύο διανυσματικοί χώροι και V^*, W^* οι αντίστοιχοι δυϊκοί τους και $f : V \to W$ μία γραμμική απεικόνιση, τότε $f^* : W^* \to V^*$ η δυϊκή απεικόνιση όπου $f^*(w) = w \circ f$.
Εάν $V = A^n, W = A^m, T_1, ..., T_m \in k[X_1, ..., X_n]$ τότε ορίζεται πολυωνυμική απεικόνιση $T : A^n \to A^m$ τ.ω $T(a_1, ..., a_n) = (T_1, ..., T_m)(a_1, ..., a_n)$. Σε αυτή την περίπτωση γράφουμε για συντομία $T = (T_1, ..., T_m)$, καθώς τα T_i ορίζονται μονοσήμαντα από την T.
Καταλήγουμε σε μία βασική πρόταση:

Πρόταση 2.2. *Έστω $V \subset A^n, W \subset A^m$ αφφινικές ποικιλότητες . Υπάρχει μία φυσική 1-1 αντιστοίχιση μεταξύ των πολυωνυμικών απεικονίσεων $\phi : V \to W$ και των ομομορφισμών $\tilde{\phi} : \Gamma(W) \to \Gamma(V)$. Κάθε τέτοια ϕ είναι ο περιορισμός μια πολυωνυμικής απεικόνισης από το A^n στο A_m.*

Η απόδειξη παραλείπεται.
Μία πολυωνυμική απεικόνιση $\phi : V \to W$ λέγεται ισομορφισμός εάν η $\tilde{\phi}$ είναι ισομορφισμός.

Εύκολα ελέγχουμε την επόμενη πρόταση

Πρόταση 2.3. *Έστω $\phi : V \to W, \psi : W \to Z$. Τότε $\widetilde{\psi \circ \phi} = \tilde{\phi} \circ \tilde{\psi}$. Η σύνθεση πολυωνυμικών απεικονίσεων είναι πολυωνυμική απεικόνιση.*

Απόδειξη. Η απόδειξη βγαίνει αμέσως από τους ορισμούς.

Έχουμε $\psi \circ \phi : V \to Z$ και $\widetilde{\psi \circ \phi} : \Gamma(Z) \to \Gamma(V), \quad \tilde{\phi} \circ \tilde{\psi} : \Gamma(Z) \to \Gamma$.

Έστω $f \in \Gamma(Z)$ Τότε $\widetilde{\psi \circ \phi}(f) = f \circ (\psi \circ \phi) = f \circ \psi \circ \phi$.

Ενώ $\tilde{\phi} \circ \tilde{\psi}(f) = \tilde{\phi} \circ (f \circ \psi) = (f \circ \psi) \circ \phi = f \circ \psi \circ \phi$.

Το ότι η σύνθεση πολυωνυμικών απεικονίσεων είναι πολυωνυμική απεικόνιση αφήνεται στον αναγνώστη(προκύπτε αμέσως πάλι από τον ορισμό γράφοντας αναλυτικά κάθε πολυωνυμική απεικόνιση). □

Είναι σημαντικό να είμαστε κάθε φορά σε θέση να κρίνουμε εάν είναι αλγεβρικό σύνολο είναι ποικιλότητα, δηλαδή εάν ένα συγκεκριμένο ιδεώδες είναι πρώτο. Παρόλάυτά ο έλεγχος αυτός δεν είναι πάντοτε εύκολος, ακόμα και αν αξιοποιούμε εργαλεία όπως βάσεις Groebner . Η επόμενη πρόταση δίνει μία χρήσιμη ικανή συνθήκη για τον έλεγχο αυτό.

Πρόταση 2.4. *Εάν $\phi : V \to W$ πολυωνυμική απεικόνιση και X αλγεβρικό υποσύνολο του W, τότε $\phi^{-1}(X)$ είναι αλγεβρικό υποσύνολο του V. Εάν $\phi^{-1}(X)$ ανάγωγο και το $X \subset \phi(V)$, τότε το X είναι ανάγωγο.*

Απόδειξη. Έστω $V \subset A^n, W \subset A^m$ και $X = V(G_1, .., G_r), G_i \in k[X_1, ..., X_m]$. Τότε $\phi^{-1}(X) = \phi^{-1}(V(G_1, ..., G_r$ Αφού φ πολυωνυμική, συνεπώς $\phi = T = (T_1, ..., T_m)$, όπου $T_i \in k[X_1, ..., X_n]$. Θεωρούμε $F_i = G_i \circ \phi = G[T_1(x_1, ..., x_n), ..., T_m(x_1, ..., x_n)], i = 1, ..., r$. Τα F_i είναι πολυώνυμα στο $k[X_1, .., X_n]$. Θεωρώ $Y = V(F_1, ..., F_r) \cap V \subset A^n$. Αρκεί να δείξουμε ότι $Y = \phi^{-1}(X)$.

$Y \subset \phi^{-1}(X)$: Έστω $y \in Y \Rightarrow F_i(y) = 0 \quad \forall i \Rightarrow G_i \circ \phi(y) = 0 \quad \forall i \Rightarrow \phi(y) \in V(G_1, ..., G_r) = X$. Άρα $\phi(Y) \subset X$.

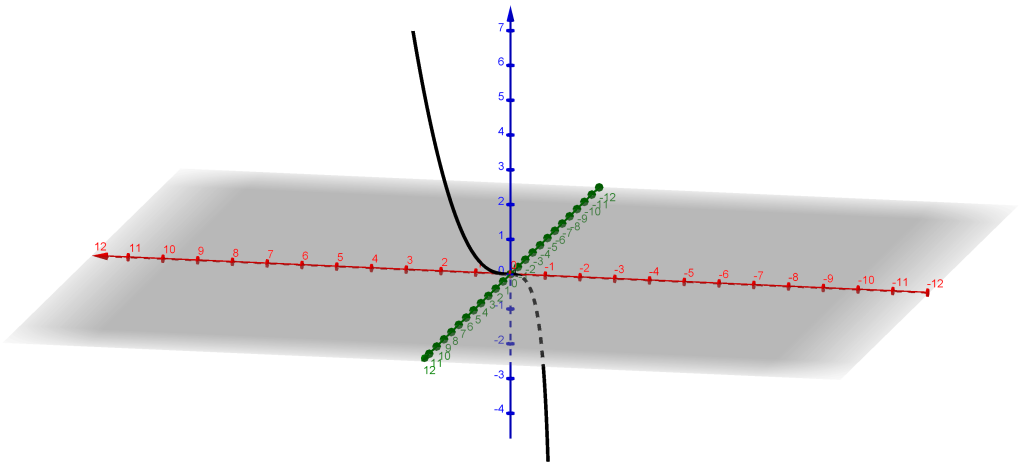
$\phi^{-1}(X) \subset Y$: Έστω $z \in \phi^{-1}(X) \Rightarrow \phi(z) \in X \Rightarrow G_i(\phi(z)) = 0 \quad \forall i \Rightarrow G_i \circ \phi(z) = 0 \Rightarrow F_i(z) = 0 \quad \forall i \Rightarrow z \in Y$ Άρα $\phi^{-1}(X) = U$.

Συνεπώς το $\phi^{-1}(X)$ είναι αλγεβρικό.

Έστω τώρα ότι $\phi^{-1}(X)$ είναι ανάγωγο κι έστω $X = X_1 \cup X_2$ όπου X_1, X_2 αλγεβρικά υποσύνολα. Τότε $\phi^{-1}(X) = \phi^{-1}(X_1) \cup \phi^{-1}(X_2)$. Όμως γνωρίζουμε από το προηγούμενο βήμα ότι $\phi^{-1}(X_1), \phi^{-1}(X_2)$ είναι αλγεβρικά και μάλιστα μη κενά αφού ϕ είναι επί από υπόθεση. Αφού όμως $\phi^{-1}(X)$ ανάγωγο συνεπώς $\phi^{-1}(X_1) = \phi^{-1}(X_2) \overset{\phi\text{επί}}{\Rightarrow} X = X_1 = X_2$. Άρα X ανάγωγο. □

Για να εκτιμήσουμε τη χρησιμότητα της πρότασης θα προσπαθήσουμε μία φαινομενικά δύσκολη εφαρμογή.

Εφαρμογή 2.1. *(a) Να δείξετε ότι το σύνολο $\{(t, t^2, t^3) \in A^3_k | t \in k\}$ είναι αφφινική ποικιλότητα (και προφανώς αλγεβρικό). Μάλιστα είναι το λεγόμενο twisted cubic .*



Σχήμα 2.1: twisted cubic

(β) Να δείξετε ότι $V = V(XZ - Y^2, YZ - X^3, Z^2 - X^2Y) \subset A^3(\mathbb{C})$ είναι ποικιλότητα. (Υπόδειξη: $Y^3 - X^4, Z^3 - X^5, Z^4 - Y^5 \in I(V)$).

Απόδειξη. (α). Έστω $A = \{(t, t^2, t^3) \in A^3_k | t \in k\}$. Εύκολα βλέπουμε ότι $A = V(Y - X^2, Z - X^3)$ και άρα αλγεβρικό (αφήνεται σαν άσκηση). Ορίζουμε $\phi : A^1_k \to V$, με $\phi(t) = (t, t^2, t^3)$. Εξ' ορισμού ϕ επί και γνωρίζουμε ότι A^1_k ανάγωγο, συνεπώς Α ανάγωγο από την προηγούμενη πρόταση.
Το δεύτερο ερώτημα είναι αρκετά πιο δύσκολο αλλά η λογική είναι η ίδια.

(β) Ονομάζουμε για ευκολία $F_1 = XZ - Y^2, F_2 = YZ - X^3, F_3 = Z^2 - X^2Y$ Όπως προτείνει η υπόδειξη, παρατηρούμε ότι $Y^3 - X^4 = -YF_1 + XF_2, Z^3 - X^5 = ZF_3 + X^2F_2, Z^4 - Y^5 = Z^2F_3 + (XYZ + Y^3)(ZX - Y^2)$ και συνεπώς ανήκουν στο $I(V)$. Μπορούμε λοιπόν να ορίσουμε μία πολυωνυμική απεικόνιση $\phi : A^1(\mathbb{C}) \to V$ με $\phi(t) = (t^3, t^4, t^5)$. Εάν συμβολίσουμε $G_1 = Y^3 - X^4, G_2 = Z^3 - X^5, G_3 = Z^4 - Y^5$ εύκολα βλέπουμε ότι οποιοδήποτε σημείο της μορφής (t^3, t^4, t^5) μηδενίζει τα G_i, F_i δηλαδή πράγματι η ϕ πάει από το A^1 στο V (και είναι καλά ορισμένη και πολυωνυμική με πολυώνυμα τα $T_1 = t^3, T_2 = t^4, T_3 = t^5$. Αρκεί να δείξουμε ότι είναι επί.
Έστω $(x, y, z) \in V$. Θέλουμε να βρούμε $t \in \mathbb{C} : (x, y, z) = (t, t^2, t^3)$. Αν $(x, y, y) = (0, 0, 0)$ τότε τετριμμένα $t = 0$. Αν όχι τότε αφού $\mathbb{C}$ αλγεβρικά κλειστό υπάρχουν 3 σε πλήθος $t \in \mathbb{C}$ τ.ω $t^3 = x$. Από τις σχέσεις $Y^3 - X^4 = 0$ και $Z^3 - X^5 = 0$ έχουμε ότι $y^3 = x^4 = t^{12}$ και $z^3 = x^5 = t^{15}$. Μετρώντας το πλήθος των λύσεων θα καταλήξουμε ότι υπάρχει t τ.ω $t^3 = x, t^4 = y, t^5 = z$, όπου $(x, y, z) \in I(V)$.
Πράγματι ήδη έχουμε ότι υπάρχουν 3 t ώστε $t^3 = x$. Όμως $t^{12} = y^3 \Rightarrow (t^4 - y)(t^8 + ty + y^2) = 0$, αλλά $t^8 = x^2t^2$. Αντικαθιστώντας το παίρνουμε ότι $(t^4 - y)(t^2x^2 + ty + y^2) = 0$. Ξέρουμε ότι 3 λύσεις ικανοποιούν αυτό το σύστημα εκ των οποίων το πολύ δύο από αυτές μπορούν να βρίσκονται στο 2ο σκέλος. Συνεπώς τουλάχιστον μία λύση βρίσκεται στο πρώτο μέρος της εξίσωσης, δηλαδή υπάρχει τουλάχιστον ένα $t \in \mathbb{C}$ ώστε $t^4 - y = y$ (και $t = x^3$). Όμοια έχουμε ότι $t^{15} - z^3 = 0 \Rightarrow (t^5 - z)(t^{10} + t^5z + z^2) = 0$. Όμως $t^{10} = x^3t, t^5 = xt^2$ άρα καταλήγουμε ότι $(t^5 - z)(tx^3 + t^2xz + z^2) = 0$. Πάλι το πολύ 2 λύσεις βρίσκονται στο 2ο σκέλος αλλά συνολικά υπάρχουν τρεις, συνεπώς υπάρχει τουλάχιστον ένα t τ.ω $(t^3, t^4, t^5) = (x, y, z)$.
Καταλήξαμε λοιπόν ότι ϕ είναι επί και άρα από την προηγούμενη πρόταση το V ποικιλότητα.
(Παρατήρηση: Θεωρήσαμε εξαρχής ότι $V_0 = V(G_1, G_2, G_3) = V$ το οποίο χρίζει όμως περισσότερης αιτιολόγησης. Έχουμε ότι $G_1, G_2, G_3 \in I(V) \Rightarrow (G_1, G_2, G_3) \subset I(V) \Rightarrow V \subset V_0$. Εν γένει η ϕ είναι μία απεικόνιση

από το $A^1(\mathbb{C})$ στο V_0 που μόλις δείξαμε ότι είναι επί. Αλλά αμέσως βλέπουμε ότι κάθε στοιχείο της μορφής $P(t^3, t^4, t^5)$ ανήκει στο V, αφού $F_1(P) = F_2(P) = F_3(P) = 0$. Συνεπώς $V_0 = V$). □

Αλλαγές Συντεταγμένων Εάν $T = (T_1, ..., T_m)$ μία πολυωνυμική απεικόνιση από το A^n στο A^m και $F \in k[X_1, ..., X_n]$ τότε ορίζουμε $F^T = \tilde{T}(F) = F(T_1, ..., T_m)$. Για ιδεώδη I και αλγεβρικά σύνολα V στο A^m αυτό μπορούμε να το γενικεύσουμε ορίζοντας I^T το ιδεώδες στο $k[X_1, ..., X_n]$ που παράγεται από τα $\{F^T | F \in I\}$, και $V^T = T^{-1}(V) = V(I^T)$, όπου $I = I(V)$. Αν V είναι υπερεπιφάνεια του F, δηλαδή $V = V(F)$, τότε $V^T = V(F^T)$ υπερεπιφάνεια του F^T (εάν F^T όχι σταθερό).
Μία αφφινική αλλαγή συντεταγμένων στο A^n είναι μία πολυωνυμική απεικόνιση $T = (T_1, ..., T_n) : A^n \to A^n$ τ.ω κάθε T_i είναι πολυώνυμο βαθμού 1 και T είναι 1-1 και επί. Αν $T_i = \sum_j a_{ij} X_j + a_i$, τότε μπορώ να σπάσω την T σε δύο μέρη, μία μετατόπιση και μία γραμμική απεικόνιση, ήτοι $T = T'' \circ T'$,όπου T' γραμμική ($T'_i = \sum_j a_{ij} X_j$) και T'' μία μετατόπιση ($T''_i = X_i + a_i$). Αφού κάθε μετατόπιση έχει αντίστροφη (που είναι επίσης μετατόπιση), συμπεραίνουμε ότι η T θα είναι 1-1 (και επί) αν-ν η T΄ είναι αντιστρέψιμη. Εάν T και U είναι αφφινικές αλλαγές συντεταγμένων στο A^n τότε και η $T \circ U, T^{-1}$ είναι αφφινικές αλλαγές συντεταγμένων. Οι αποδείξεις είναι προφανείς από τους ορισμούς. Ο T λοιπόν είναι ένας ισομορφισμός της ποικιλότητας A^n με τον εαυτό του.

Ορισμός 2.2. *Ένα σύνολο $V \subset A^n$ λέγεται γραμμική υποποικιλότητα του A^n_k εάν $V = V(F_1, ..., F_r)$ όπου F_i πολυώνυμα 1ου βαθμού.*

Οι ευθείες και γενικά οι γραμμικές ποικιλότητες είναι τα πιο απλά παραδείγματα ποικιλοτήτων που μπορούμε να μελετήσουμε. Στην επόμενη πρόταση/άσκηση θα δούμε ότι η κλάση των γραμμικών ποικιλοτήτων παραμένει αναλλοίωτη μέσα από αφφινικές αλλαγές συντεταγμένων και έπειτα θα εισάγουμε την έννοια της διάστασης την οποία θα γενικεύσουμε σε επόμενο κεφάλαιο.

Πρόταση 2.5. *(α) Εάν T αφφινική αλλαγή συντεταγμένων και V ένα γραμμική υποποικιλότητα, τότε το V^T παραμένει γραμμική υποποικιλότητα*
(β) Αν $V \neq 0$ τότε υπάρχει αλλαγή συντεταγμένων T του A^n τ.ς $V^T = V(X_{m+1}, ..., X_n)$. Συνεπώς το V είναι ποικιλότητα.
(γ) Το m αυτό που εμφανίζεται στο προηγούμενο βήμα είναι ανεξάρτητο της επιλογής του T. Λέγεται διάσταση του V. Τότε το V είναι ισόμορφο με το A^m_k.

Απόδειξη. (α) Εύκολα βλέπουμε ότι εάν $V = V(F_1, ..., F_r)$ τότε $V^T = V((F_1)^T, (F_2)^2, ..., (F_r)^T)$. Αρκεί λοιπόν να δείξουμε ότι εάν $\deg F = 1 \Rightarrow \deg(F^T) = 1$
Όμως $\deg(F) = 1 \Rightarrow F = \sum_j a_j X_j + b$ και $a_j \neq 0$ για κάποιο j. Έστω $T = T_1, ..., T_n$ αφφινική αλλαγή συντεταγμένων
Συνεπώς, $F^T = \sum_j a_j(T_j(X_1, ..., X_n)) + b = \sum_j a_j(\sum_i c_{ij} X_i + d_j) + b$ και $c_{ij} \neq 0$ για κάποιο i (για κάθε j υπάρχει ένα τέτοιο i).
Άρα $F^T = \sum_j(\sum_i(a_j c_{ij} X_i)) + \sum_j(a_j + d_j) + b$. Όμως T αφφινική αλλαγή συντεταγμένων και άρα ο πίνακας $A = [c_{ij}]$, έχει μη μηδενική ορίζουσα, και συνεπώς $= \sum_j(\sum_i(a_j c_{ij} X_i)) = 0 \Leftrightarrow a_j = 0 \forall j$. Όμως υπάρχει κάποιο j τ.ω $a_j \neq 0$ και άρα το πολυώνυμο F^T εν τέλει είναι όντως πρώτου βαθμού.

(β) $V = V(F_1, ..., F_r) \neq 0$ Θα δείξουμε το ζητούμενο με επαγωγή στο r.
Για $r = 1$, $V = V(F)$. Έστω χ.β.γ ότι $F = a_1 X_1 + ... + a_n X_n + a_0, a_1 \neq 0$. Τότε θεωρώ $T = (T_1, ..., T_n)$ τ.ω $T_1 = \frac{1}{a_1} X_1 - \frac{a_0}{a_1}, T_i = X_i$ αν $a_i = 0$, $T_j = \frac{1}{a_j} X_j$ και $T_j = \frac{1}{a_j} X_j$ αν $a_j \neq 0$

Τότε $F^T = X_1 + \delta_i X_i$, όπου $d_i = \begin{cases} 0 & \text{αν} \quad a_i = 0 \\ 1 & \text{αν} \quad a_i \neq 0 \end{cases}$

Τότε για $U = (U_1, ..., U_n)$,όπου $U_1 = X_1 = \sum_i \delta_i X_i$, $U_i = X_i$ για $i = 2, ..., n$ έχουμε ότι $F^{U \circ T} = X_1$ και $\deg U_i = 1$ άρα αντιστρέψιμος, άρα είναι αλλαγή συντεταγμένων.
Συνεπώς $V(F^{U \circ T}) = V(X_1)$.

(β) Έστω ότι ισχύει για $V = V(F_1, ..., F_r)$ κι έστω $V = V(F_1, ..., F_r, F_{r+1})$. Τότε $V = V(F_1) \cap V(F_2, ..., F_{r+1}) \overset{\text{επαγωγή}}{=} V(F_1^T) \cap V(X_{m+1}, ..., X_n) = V(F_1^T, X_{m+1}, ..., X_n)$
Σπάμε την F_1 ως εξής: $F_1 = G + \sum_{i=m+1}^{n} b_i X_i$,όπου $G = \sum_{i=1}^{m} X_i + b_0$. Τότε $V(F_1, X_{m+1}, ..., X_n) = V(G, X_{m+1}, ..., X_n)$ Εάν $G = 0$ έχουμε τελειώσει. Εάν όχι, τότε θεωρούμε $U = (U_1, ..., U_m)$ τ.ω $G^U = V(X_m)$ (μπορούμε να το κάνουμε από υπόθεση επαγωγής, αφού $G \in k[X_1, ..., X_m]$ πρώτου βαθμού). Επεκτείνουμε την U σε όλον τον χώρο ορίζοντας $U_i = X_i \quad \forall i \geq m+1$ Τότε εύκολα βλέπουμε ότι $V^{U \circ T} = V(X_m, ..., X_n)$ όπως θέλαμε.

(γ) Έστω ότι υπάρχει αφφινική αλλαγή συντεταγμένων T τ.ω $V(X_{m+1}, ..., X_n)^T = V(X_{s+1}, ..., X_s)$ με $s \neq m$ Έχουμε ότι $V(X_{m+1}, ..., X_n)^T = V(X_{m+1}^T, ..., X_n^T = V(T_m + 1), ..., T_n) = V(X_{s+1}, ..., X_n) = \{(a_1, ..., a_s, 0, ..., 0), a_i \in k\} = V$.
Άρα $\forall x \in V \Rightarrow T_{m+i}(x) = 0 \Rightarrow T_{m+i} \in k[X_{s+1}, ..., X_n], i = 1, ..., n-m$ Όμως $B = \{X_{s+1}, ..., X_n\}$ είναι βάση του $I(V)$ ενώ τα $\{T_{m+i}\}$ είναι διαφορετικά σε πλήθος από s . Εάν είναι περισσότερα σε πλήθος, σημαίνει ότι είναι γραμμικά εξαρτημένα και άρα Τ όχι αφφινική αλλαγή συντεταγμένων, ενώ εάν είναι λιγότερα σε πλήθος, τότε δεν παράγουν όλο το ιδεώδες.

Για μία γενική γραμμική ποικιλότητα εάν υπάρχουν U, T αφφινικές αλλαγές συντεταγμένων τ.ω $V^T = V(X_{m+1}, ..., X_n), V^U = V(X_{s+1}, ..., X_n)$, τότε $(V^T)^{T^{-1} \circ U} = V(X_{s+1}, ..., X_n)$ που είναι άτοπο από τα προηγούμενα. □

Κοιτώντας την απόδειξη, παρατηρούμε ότι το υπερεπίπεδο είναι διάστασης $n-1$. Γενικά ισχύει ότι οποιαδήποτε υπερεπιφάνεια είναι διάστασης 1 αλλά αυτό θα το δούμε πιο αυστηρά στα επόμενα κεφάλαια.

Θα δούμε συγκεκριμένα κι ένα παράδειγμα με ευθείες που θα μας χρησιμεύσει αρκετά παρακάτω. Καταρχάς να ορίσουμε αυστηρά την ευθεία:

Ορισμός 2.3. *Έστω $P = (a_1, ..., a_n), Q = (b_1, ..., b_n)$ διακεκριμένα σημεία του A^n. Η ευθεία που περνάει από τα P, Q ορίζεται ως η $\{(a_1 + t(b_1 - a_1), ..., a_n + t(b_n - a_n)) | t \in k\}$*

Ακολουθεί η άσκηση/πρόταση.

Πρόταση 2.6. *(α) Αν L η ευθεία που περνάει από τα P, Q και T αφφινική αλλαγή συντεταγμένων, τότε η $T(L)$ είναι η ευθεία που περνάει από τα $T(P), T(Q)$*
(β) Η ευθεία είναι γραμμική ποικιλότητα διάστασης 1 αλλά και αντίστροφα μία γραμμική υποποικιλότητα διάστασης 1 αποτελεί ευθεία που περνά από οποιαδήποτε δύο της σημεία.
(γ) Στον A^2 η ευθεία ταυτίζεται με το υπερεπίπεδο.
(δ) Έστω $P, P' \in A^2, L_1, L_2$ δύο διακεκριμένες ευθείες που περνάνε από το P και L_1', L_2' δύο διακεκριμένες ευθείες που περνάνε από το P'. Τότε υπάρχει αφφινική αλλαγή συντεταγμένων T του A^2 τ.ω $T(P) = P'$ και $T(L_i) = L_i', i = 1, 2$.

Απόδειξη. Έστω $T = (T_1, ..., T_n), T_i = \sum_j a_{ij} X_j + a_{i0}$.
Οπότε $T(P) = (T_1(P), ..., T_n(P)), T(Q) = (T_1(Q), ..., T_n(Q))$ και

$$T(L) = (T_1(L), ..., T_n(L) = \{(\sum a_{ij}(a_j + t(b_j - a_j)) + a10, ..., \sum a_{nj}(a_j + t(b_j - a_j)) + a_{n0})\} =$$

$$= T(P) + t(T(Q) - T(P)$$

(β) Έστω L μία ευθεία που περνάει από το P και το Q. Από το προηγούμενο ερώτημα, αντί να δουλεύουμε με όλη την ευθεία, αρκεί απλά να δουλεύουμε με τα δυο της σημεία P, Q. Θέλουμε να στείλουμε το P στο $(0, ..., 0)$ και το Q στο $(1, 0, ..., 0)$. Εφαρμόζουμε αφφινική αλλαγή συντεταγμένων $T = (X_1 - a_1, ..., X_n - a_n)$ που στέλνει το P στο $(0, ...0,)$. Έστω ότι $T(Q) = (q_1, ..., q_n)$ Προφανώς $T(Q) \neq (0, ..., 0)$ οπότε υπάρχει κάποιο $q_i \neq 0$. Χ.β.γ υποθέτουμε $q_1 \neq 0$ Τότε εφαρμόζουμε $U = (U_1, ..., U_n)$, $U_1 = \frac{1}{q_1})X_1$, $U_i = q_i X_1 - q_1 X_i, i > 1$.
Η $T' = U \circ T$ είναι αφφινική αλλαγή συντεταγμένων ως σύνθεση και έχει την επιθυμητή ιδιότητα που θέλαμε.

Συνεπώς $T'(L) = \{(t, 0, ..., 0) | t \in k\} = V(X_2, ..., X_n)$ και άρα είναι γραμμική υποποικιλότητα διάστασης 1.
Αντίθετα, έστω L μία γραμμική υποποικιλότητα διάστασης 1. Τότε υπάρχει αφφινική αλλαγή συντεταγμένων T τέτοια ώστε $L^{=}V(X_2, ..., X_n)$ όπου προφανώς είναι ευθεία (η ευθεία που περνάει από τα $(0, ..., 0)$ και $(1, ..., 0)$)
(γ) Προκύπτει αμέσως από το (β) αφού $L^T = V(Y)$ υπό κατάλληλη αφφινική αλλαγή συντ/νων.
(δ) Όπως είδαμε οι αφφινικές αλλαγές συντεταγμένων αφήνουν αναλλοίωτα τα πάντα οπότε μπορούμε ανέκαθεν σε τέτοιου είδους ασκήσεις να θεωρούμε, χωρίς βλάβη της γενικότητας, οποιοδήποτε σημείο ή οποιαδήποτε ευθεία θέλουμε. Εδώ για παράδειγμα για απλούστευση διαλέγουμε χ.β.γ $P' = (0, 0), L'_1 = X, L'_2 = Y$ και θέλουμε λοιπόν να βρούμε μία αλλαγή συντεταγμένων τ.ω $T(P) = (0, 0), T(L_1) = X, T(L_2) = Y$. Από το προηγούμενο ερώτημα μπορούμε να βρούμε U αφφινική αλλαγή συντεταγμένων ώστε $U(P) = 0$ και $U(L_1) = X$, δηλαδή να υπάρχει $Q \in L_1 : U(Q) = (0, 1)$ Έστω $N = (n_1, n_2) \in L_2^U$ και προφανώς $n_2 \neq 0$ αν $n_1 \neq 0$ γιατί τότε η L_2^U θα ταυτίζεται με την L_1^U. Διαλέγουμε $N\ neq(0, 0)$ και άρα $n_2 \neq 0$ και φτιάχνουμε την αλλαγή συντεταγμένων $T = (T_1, T_2), T_2 = \frac{1}{n_2}Y, T_1 = n_2X - n_1Y$. Εύκολα βλέπουμε ότι η $T \circ U$ είναι η επιθυμητή αλλαγή συντεταγμένων. □

2.2 Ρητές συναρτήσεις, τοπικοί δακτύλιοι και ΔΔΕ

Επόμενος στόχος είναι να μελετήσουμε το σώμα κλασμάτων του $\Gamma(V)$ από το οποίο όπως θα δούμε θα προκύψει η έννοια του τοπικού δακτυλίου. Οι τοπικοί δακτύλιοι μας ενδιαφέρουν αρκετά, καθώς είναι σχετικά απλοί στον χειρισμό τους και μας βοηθάνε να μελετήσουμε αυτό που ονομάζουμε ¨τοπική συμπεριφορά¨.

Ας δώσουμε αυστηρά τον ακόλουθο ορισμό.

Ορισμός 2.4. *Έστω V ποικιλότητα στο A_k^n και $\Gamma(V)$ ο δακτύλιος συντεταγμένων (Θυμίζουμε ότι $I(V)$ πρώτο ιδεώδες, και άρα $\Gamma(V)$ ακεραία περιοχή). Ονομάζουμε σώμα ρητών συναρτήσεων του V και το συμβολίζουμε με $k(V)$ το σώμα κλασμάτων του $\Gamma(V)$. Ένα στοιχείο του $k(V)$ λέγεται ρητή συνάρτηση στο V.*

Αν f μία τέτοια ρητή συνάρτηση στο V και $P \in V$, τότε λέμε ότι η f ορίζεται στο P αν για κάποια $a, b \in \Gamma(V), f = \frac{a}{b}, b(P) \neq 0$. Παρατηρείστε ότι υπάρχουν πολλοί τρόποι που μπορεί να γραφτεί η f ως κλάσμα δύο ρητών συναρτήσεων. Η f ορίζεται στο P αν μπορούμε να βρούμε έναν τέτοιο τρόπο, ώστε ο παρανομαστής της f να μην μηδενίζεται στο P. Αν όμως, $\Gamma(V)$ είναι Π.Μ.Α τότε ουσιαστικά υπάρχει μοναδικός τρόπος γραφής της f ως $f = \frac{a}{b}$ όπου a, bνα μην έχουν κοινούς παράγοντες και άρα τότε η f ορίζεται στο P αν-ν $b(P) \neq 0$.

Ας δούμε ένα παράδειγμα για να το καταλάβουμε καλύτερα.
Παράδειγμα : Έστω $V = V(XW - YZ) \subset A_k^4, \Gamma(V) = k[X, Y, Z, W]/(XW - YZ)$. Έστω $\bar{X}, \bar{Y}, \bar{Z}, \bar{W}$ οι εικόνες (residues) των X, Y, Z, W στο $\Gamma(V)$. Τότε $f = \frac{\bar{X}}{\bar{Y}} = \frac{\bar{Z}}{\bar{W}} \in k(V)$ ορίζεται στο $P = (x, y, z, w) \in V$ αν $y \neq 0$ ή $w \neq 0$.

Η τοπικοποίηση του δακτυλίου προκύπτει σε κάθε σήμειο εάν πάρουμε μόνο τις συναρτήσεις που ορίζονται σε αυτό το σημείο. Συγκεκριμένα, εάν $P \in V$, ορίζουμε $\mathcal{O}_P(V)$ το σύνολο όλων των ρητών συναρτήσεων του V που ορίζονται στο P. Κατευθείαν βλέπουμε ότι το $\mathcal{O}_P(V)$ σχηματίζει υποδακτύλιο του $k(V)$ που περιέχει το $\Gamma(V)$: $k \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset k(V)$.
Ο $\mathcal{O}_P(V)$ λέγεται τοπικός δακτύλιος του V στο P .
Το σύνολο των σημείων όπου δεν ορίζεται μία ρητή συνάρτηση f λέγεται πόλος της f .

Πρόταση 2.7. *1. Ο πόλος μιας ρητής συνάρτησης f στο V είναι αλγεβρικό υποσύνολο του V*

2. $\Gamma = \bigcap_{P \in V} \mathcal{O}_P(V)$

Απόδειξη. Έστω $V \subset A^n$. Για $G \in k[X_1, ..., X_n]$ γράφουμε με $\bar{G}$ την εικόνα του στο $\Gamma(V)$. Έστω $f \in k(V)$. Έστω $J_f = \{G \in k[X_1, ..., X_n] | \bar{G}f \in \Gamma(V)\}$. Θα δείξουμε ότι είναι ιδεώδες.
Αν $G \in J_f, H \in k[X_1, ..., X_n]$ τότε $\overline{GH}f = \bar{G}\bar{H}f = (\bar{G}f)\bar{H} \in \Gamma \Rightarrow GH \in J_f$. Όμοια, αν $G, H \in J_f \Rightarrow \overline{G-H}f = \bar{G}f - \bar{H}f \in \Gamma(V) \Rightarrow G - H \in J_f$. Άρα είναι όντως ιδεώδες.
Τα σημεία του είναι ακριβώς τα σημεία στα οποία δεν ορίζεται η f, αφού $V(J_f) = \{P \in A_k^n\} : G(P) = 0 \forall G \in J_f$. Όμως $\bar{G}f \in \Gamma(V)$. Αν γράψω την f ως $f = \dfrac{a}{b}, a, b \in \Gamma(V)$ τότε $\bar{G}f = \bar{G}\dfrac{a}{b} \in G(V) \Rightarrow \forall P \in V : b(P) = 0$ ισχύει ότι $G(P) = 0$ (θεωρούμε ότι a, b δεν έχουν κοινούς παράγοντες) και άρα δείξαμε το πρώτο κομμάτι.
Αν $f \in \cap_{P \in V} \mathcal{O}_P(V)$ τότε $V(J_f) = \emptyset$ και άρα από το Nullstellensatz έχουμε ότι $J_f = k[X_1, ..., X_n]$, δηλαδή $1 \in J_f \Rightarrow \bar{1}f = f \in \Gamma(V)$ που αποδυκνύει το δεύτερο κομμάτι. □

Γενικά στην αντιμεταθετική άλγεβρα, τοπικός είναι ο δακτύλιος που έχει μοναδικό μέγιστο ιδεώδες(Γενικά κάθε δακτύλιος έχει μέγιστα ιδεώδη, γεγονός που προκύπτει σχετικά εύκολα από το λήμμα του Zorn). Θα προσπαθήσουμε λοιπόν να δικαιολογήσουμε γιατί ο $\mathcal{O}_P(V)$ ονομάστηκε τοπικός δακτύλιος του V στο P.

Έστω $f \in \mathcal{O}_P(V)$. Τότε (και μόνο τότε), μπορούμε να ορίσουμε την τιμή της f στο P, συμβολικά $f(P)$, ως εξής : Γράφουμε την f ως $f = \dfrac{a}{b}, a, b \in \Gamma(V), b(P) \neq 0$ και ορίζουμε $f(P) = \dfrac{a(P)}{b(P)}$. Εύκολα βλέπουμε ότι αυτός ο ορισμός είναι ανεξάρτητος της επιλογής των a, b δηλαδή είναι καλά ορισμένος. Ονομάζουμε τότε $M_P(V) = \{f \in \mathcal{O}_P(V) | f(P) = 0\}$ <u>το μέγιστο ιδεώδες</u> του V στο P. Αποτελεί τον πυρήνα του ομομορφισμού εκτίμησης $\phi : \mathcal{O}_P(V) \to k, f \mapsto f(P)$ και συνεπώς $\mathcal{O}_P(V)/M_p(V) \cong k$ (ο έλεγχος είναι ξεκάθαρος από τον ορισμό κατευθείαν). Ένα στοιχείο $f \in \mathcal{O}_P(V)$ λέγεται μονάδα στο $\mathcal{O}_P(V)$ αν-ν $f(P) \neq 0$, δηλαδή $M_P(V) = \{$μη μονάδες του$\mathcal{O}_P(V)\}$. Παρατηρούμε ότι κάθε μονάδα είναι αντιστρέψιμο στοιχείο στο $\mathcal{O}_P(V)$ (εξού και η ονομασία του). Όμως γνωρίζουμε από την άλγεβρα την εξής πρόταση:

Πρόταση 2.8. *Για έναν δακτύλιο R τα ακόλουθα είναι ισοδύναμα:*

1. *Το σύνολο των μη αντιστρέψιμων στοιχείων του R είναι ιδεώδες.*
2. *Ο R έχει μοναδικό μέγιστο ιδεώδες που περιέχει κάθε άλλο γνήσιο ιδεώδες του R*

Η απόδειξη είναι προφανής. Αν $M =\{$μη μονάδες$\}$, τότε προφανώς κάθε ιδεώδες του R περιέχεται στο M Όμως, αφού το $M_P(V)$ αποτελεί πυρήνα ομομορφισμού, άρα είναι ιδεώδες και συνεπώς είναι το μοναδικό μέγιστο ιδεώδες του $\mathcal{O}_P(V)$. Συνεπώς ο $\mathcal{O}_P(V)$ πράγματι είναι τοπικός δακτύλιος, με $M_P(V)$ το μοναδικό μέγιστο ιδεώδες του.
Ισχύει όμως και κάτι παραπάνω για τον $\mathcal{O}_P(V)$.

Πρόταση 2.9. *Ο $\mathcal{O}_P(V)$ είναι Noetherian τοπική ακεραία περιοχή.*

Η απόδειξη είναι αρκετά σημαντική ως μεθοδολογία καθώς μας βοηθά να διευκρινήσουμε κάποιες έννοιες

Απόδειξη. Αρκεί να δείξουμε ότι κάθε ιδεώδες I του $\mathcal{O}_P(V)$ είναι πεπερασμένα παραγόμενο. Έστω λοιπόν I ένα τέτοιο ιδεώδες
Αφού $\Gamma(V)$ είναι Noetherian και $I \cap \Gamma(V)$ είναι ιδεώδες του $\Gamma(V)$ (γιατί;) είναι πεπερασμένα παραγόμενα και άρα μπορώ να βρω $f_1, ..., f_r$ που να το παράγουν. Ισχυρίζομαι ότι τα $f_1, ..., f_r$ παράγουν το I ως ιδεώδες του $\Gamma(V)$
<u>Προσοχή</u> Στο $\Gamma(V)$, το σύνολο $(f_1, ..., f_r)$ είναι το σύνολο με στοιχεία της μορφής $\sum_{i=1}^r f_i g_i, g_i \in \Gamma(V)$, ενώ στο $\mathcal{O}_P(V)$ είναι το σύνολο με στοιχεία της μορφής $\sum_{i=1}^r f_i h_i, h_i \in \mathcal{O}_P(V)$ Συνεπώς το σύνολο $(f_1, ..., f_r)$ είναι διαφορετικό όταν αναφερόμαστε στο $\Gamma(V)$ ή στο $\mathcal{O}_P(V)$.
Αν $f \in I \subset \mathcal{O}_P(V)$ τότε υπάρχει $b \in \Gamma(V)$, με $b(P) \neq 0$ και $bf \in \Gamma(V)$. Τότε όμως $bf \in I \cap \Gamma(V)$ και άρα $bf = \sum a_i f_i, a_i \in \Gamma(V)$ και άρα $f = \sum (\frac{a_i}{b}) f_i$ όπως θέλαμε. □

Πρόταση 2.10. *Έστω $\phi : V \to W$ πολυωνυμική απεικόνιση αφφινικών ποικιλοτήτων, και $\tilde{\phi} : \Gamma(W) \to \Gamma(V)$ η επαγώμενη απεικόνιση. Έστω $P \in V, \phi(P) = Q$ τότε η $\tilde{\phi}$ επεκτείνεται μοναδικά σε ομομορφισμό δακτυλίων (που επίσης συμβολίζεται με $\tilde{\phi}$) από το $\mathcal{O}_Q(W)$ στο $\mathcal{O}_P(V)$. Μάλιστα ισχύει $\tilde{\phi}(M_Q(W)) \subset M_P(V)$*

Απόδειξη. Θυμίζουμε $\tilde{\phi} : \Gamma(W) \to \Gamma(V)$,
$tilde\phi(f) = f \circ f$.

Επεκτείνουμε την $\tilde{\phi}$ ως εξής:

$\tilde{\phi} : \mathcal{O}_Q(W) \to \mathcal{O}_P(V), f = \frac{a}{b} \mapsto \frac{\tilde{\phi}(a)}{\tilde{\phi}(b)}$. Το ότι είναι ομομορφισμός είναι προφανές. <u>Καλά ορισμένος</u>:

Έστω $f = \frac{a}{b} = \frac{c}{d}$. Τότε $ad = bc$ και $ad, bc \in \Gamma(W) \Rightarrow \tilde{\phi}(ad) = \tilde{\phi}(bc) \overset{\tilde{\phi}\text{ομομ.}}{\Rightarrow} \tilde{\phi}(b)\tilde{\phi}(c) = \tilde{\phi}(a)\tilde{\phi}(d) \Rightarrow \dfrac{\tilde{\phi}(a)}{\tilde{\phi}(b)} = \dfrac{\tilde{\phi}(c)}{\tilde{\phi}(d)}$

Επίσης $\tilde{\phi}(f) \in \mathcal{O}_P(V)$. Πράγματι εάν $f = \frac{a}{b} \in \mathcal{O}_Q(W) \not\Leftarrow b(Q) \neq 0$. Όμως $\tilde{\phi}(f) \in \mathcal{O}_P(V) \Leftrightarrow \tilde{\phi}(b)(P) \neq 0$ όπου $\tilde{\phi}(b)(P) = b \circ \phi(P) = b(Q) \neq 0$, άρα $\tilde{\phi}(f) \in \mathcal{O}_P(V)$

<u>Μοναδικότητα</u> Έστω $\tilde{\psi} : \mathcal{O}_Q(W) \to \mathcal{O}_P(V)$ μια δεύτερη επέκταση, δηλαδή $\tilde{\psi}|_{\Gamma(W)} = \tilde{\phi}|_{\Gamma(W)}$.
Θέλουμε να δείξουμε ότι $\tilde{\phi} = \tilde{\psi}$

Έστω $f = \frac{a}{b} \in \mathcal{O}_Q(W)$. Τότε $\tilde{\psi}(\frac{a}{b}) \overset{\tilde{\psi}\text{ομομ.}}{=} \tilde{\psi}(a)\tilde{\phi}(\frac{1}{b}) = \tilde{\psi}(a)\tilde{\psi}(b^{-1}) \overset{\text{ομομ}}{=} \tilde{\psi}(a)\tilde{\psi}(b)^{-1} = \dfrac{\tilde{\psi(a)}}{\tilde{\psi}(b)} \overset{\tilde{\phi}=\tilde{\psi}}{=} \frac{\tilde{\phi}(a)}{\tilde{\phi}(b)} = \tilde{\phi}(f)$ □

Παραθέτουμε τέλος μία πρόταση που θα μας χρειαστεί παρακάτω.

Πρόταση 2.11. *Έστω $T = A^n \to A^n$ αφφινική αλλαγή συντεταγμένων, $T(P) = Q$. Να δείξετε ότι $\tilde{T} : \mathcal{O}_Q(A^n) \to \mathcal{O}_P(V)$ είναι ισομορφισμός. Να δείξετε ότι η $\tilde{T}$ επάγει έναν ισομορφισμό από το $\mathcal{O}_Q(V^T)$ στο $\mathcal{O}_P(V)$ αν $P \in V$*

Απόδειξη. Από την προηγούμενη πρόταση έχουμε ότι η $\tilde{T}$ ορίζεται μονοσήμαντα από την T. Συνεπώς οι $\tilde{T} : \mathcal{O}_Q(A^n) \to \mathcal{O}_P(A^n)$ και $\tilde{T^{-1}} : \mathcal{O}_P(A^n) \to \mathcal{O}_Q(A^n)$ είναι καλά ορισμένες. Από την πρόταση 15 έχουμε ότι $\tilde{T} \circ \tilde{T^{-1}} = \widetilde{T^{-1} \circ T} = 1_{\mathcal{O}_P(A^n)}$ Όμοια και $\tilde{T^{-1}} \circ \tilde{T} = 1_{\mathcal{O}_Q(A^n)}$. Άρα $\tilde{T}$ ισομορφισμός.
Αν περιορίσουμε την $\tilde{T}$ στο $\mathcal{O}_Q(V^T)$ και την $\tilde{T^{-1}}$ στο $\mathcal{O}_P(V)$, τότε $\tilde{T} \circ \tilde{T^{-1}} = 1_{\mathcal{O}_P(V)}$ και $\tilde{T^{-1}} \circ \tilde{T} = 1_{\mathcal{O}_Q(V^T)}$ και άρα $\tilde{T}$ ισομορφισμός από το $\mathcal{O}_Q(V^T)$ στο $\mathcal{O}_P(V)$. □

Ένας άλλος, ωραίος τρόπος να σκεφτούμε τους τοπικούς δακτυλίους είναι ως δυναμοσειρές. Δεν θα επιμείνουμε σε αυτό αλλά επιγραμματικά αναφέρουμε ότι για $P = (0, ..., 0)$, $\mathcal{O}_P(A^n) = k[[X_1, ..., X_n]]$, όπου με $k[[X_1, ..., X_n]]$ συμβολίζουμε το σύνολο των δυναμοσειρών με μεταβλητές τα $X_1, .., X_n$.

Δακτύλιοι Διακριτής Εκτίμησης Οι τοπικοί δακτύλιοι από μόνοι τους είναι ήδη 'καλοί' δακτύλιοι αλλά υπάρχει μία συγκεκριμένη υποκατηγορία τους που θα μας απασχολήσει παρακάτω. Αυτοί είναι οι δακτύλιοι διακριτής εκτίμησης (ΔΔΕ) (Discrete Valuation Rings, DVRs) οι οποίοι πέρα από τοπικοί, είναι και ΠΚΙ.

Ορισμός 2.5. *Έστω R ακεραία περιοχή που δεν είναι σώμα. Ο R θα λέγεται ΔΔΕ εάν είναι Noetherian , τοπικός, και το μέγιστο ιδεώδες του είναι κύριο.*

Ο λόγος που μας ενδιαφέρουν αυτοί οι δακτύλιοι είναι εξαιτίας της επόμενης πρότασης, η οποία μας δίνει έναν εύκολο τρόπο να χαρακτηρίζουμε κάθε στοιχείο του δακτυλίου.

Πρόταση 2.12. *Έστω R ακεραία περιοχή, όχι σώμα. Τα επόμενα είναι ισοδύναμα.*

1. *Ο R είναι Noetherian τοπικός και το μέγιστο ιδεώδες είναι κύριο.*

2. *Υπάρχει ένα ανάγωγο στοιχείο $t \in R$ τ.ω κάθε μη μηδενικό στοιχείο $z \in R$ μπορεί να γραφεί με μοναδικό τρόπο ως $z = ut^n$, όπου u μονάδα στο R και n μη αρνητικός ακέραιος.*

Η απόδειξη είναι αρκετά άμεση.

Απόδειξη. (1) $\Rightarrow$ (2) : Έστω M το μέγιστο ιδεώδες και $M = (t)$, δηλαδή t ο γεννήτοράς του. Αρχικά θα δείξουμε την μοναδικότητα της γραφής. Πράγματι, εάν $ut^n = vt^m, u, v$ μονάδες, τότε $ut^{n-m} = v$ επίσης μονάδα, συνεπώς αναγκαστικά $n = m$ και $u = v$, καθώς αν υπήρχε δείκτης k ώστε t^k να είναι μονάδα, τότε $M = R$ και άρα όχι μέγιστο ιδεώδες.
Μένει να δείξουμε ότι κάθε στοιχείο μπορεί όντως να γραφεί σε αυτή τη μορφή. Προφανώς για αντιστρέφιμα στοιχεία ισχύει, αφού $u = ut^0$. Εάν z όχι μονάδα τότε $z = z_1t, z_1 \in R$. Εάν z_1 μονάδα έχουμε τελειώσει. Εάν όχι, τότε $z_1 = z_2t$ και συνεχίζουμε επαγωγικά βρίσκοντας μία ακολουθία $z_1, z_2, ...$ Έστω ότι αυτή η ακολουθία είναι άπειρη, δηλαδή η διαδικασία δεν τελειώνει ποτέ. Δημιουργείται έτσι μία αύξουσα ακολουθία ιδεωδών $(z_1) \subset (z_2) \subset ...$ η οποία, επειδή ο δακτύλιος είναι Noetherian πρέπει να έχει ένα μέγιστο στοιχείο και συνεπώς να σταματά για κάποιο n, δηλαδή $(z_n) = (z_{n+1})$. Αυτό σημαίνει ότι $z_{n+1} = vz_n$ για κάποιο $v \in R$ και άρα $z_n = vtz_n$ και άρα, επειδή είμαστε σε ακεραία περιοχή και $z_n \neq 0$, άρα $vt = 1$. Όμως t όχι μονάδα, καταλήγοντας σε άτοπο.
(2) $\Rightarrow$ (1) : (Δεν την πολυχρειαζόμαστε αυτή την κατεύθυνση). Εάν θέσω $M = (t)$, τότε το M αποτελείται από τα μη αντιστρέψιμα στοιχεία. Πράγματι, εάν u μονάδα, τότε $u = ut^0$ και αυτή η γραφή είναι μοναδική, άρα $u \notin (t) = M$. Όμοια, εάν z μη αντιστρέψιμο, προφανώς $z = ut^n, n \geq 1 \Rightarrow z \in (t) = M$. Το M είναι ιδεώδες. Πράγματι, εάν $z \in M \Rightarrow z = ut^n, n \geq 1$ και $p \in R$. Τότε $p = vt^m, m \geq 0 \Rightarrow zp = uvt^{n+m}, n + m \geq 1 \Rightarrow zp \in M$. Εάν $z, p \in M \Rightarrow z = ut^n, n \geq 1, p = vt^m, m \geq 0$. Χ.β.γ υποθέτουμε ότι $n \geq m$. Τότε $z - p = ut^n - vt^m = ut^mt^{n-m} - vt^m = t^m(ut^{n-m} - v)$. Αρκεί λοιπόν να δείξουμε ότι $(ut^{n-m} - v)$ είναι αντιστρέψιμο. Εάν $n = m$ έχουμε τελείωσει. Έστω λοιπόν $n - m = k > 0$. Τότε από υπόθεση, $ut^k - v = wt^a, a \geq 0$. Θέλουμε να δείξουμε ότι $a = 0$. Έστω $a > 0$ κι ότι $a \geq k$. Τότε $v = ut^k - wt^a = t^k(u - wt^{a-k})$. Όμως t όχι αντιστρέψιμο, άρα $v = (u - wt^{a-k}) = 0$. Αφού $v = 0$ συνεπώς $p = 0$ και άρα τετριμένα έχουμε τελειώσει Άρα ο R είναι τοπικός και το μέγιστο ιδεώδες είναι κύριο.
Μάλιστα είναι ΠΚΙ. Έστω I ιδεώδες. Τότε το I δεν περιέχει μονάδες και συνεπώς κάθε στοιχείο του I πέραν του μηδενικού είναι της μορφής ut^n. Έστω m ο μικρότερος βαθμός για τον οποίον υπάρχει στοιχείο z του I τ.ω $z = ut^m$ για κάποιο u αντιστρέψιμο. Ισχυρίζομαι ότι $I = (t^m)$. Πράγματι, $ut^m \in I \Rightarrow u^{-1}ut^m = t^m \in I \Rightarrow (t^m) \subset I$. Προφανώς όμως $I \subset (t^m)$ γιατί αλλιώς θα υπήρχε $x \in I : x = vt^l, l < m$ που είναι άτοπο. Συνεπώς το I είναι κύριο, και άρα ο R είναι ΠΚΙ. □

Από το δεύτερο σκέλος της απόδειξης παρατηρούμε ότι το να απαιτήσουμε το μέγιστο ιδεώδες να είναι κύριο ισοδυναμεί με το να ισχυριστούμε ότι ολόκληρος ο δακτύλιος είναι ΠΚΙ. Κατά κάποιον τρόπο, μπορούμε να σκεφτόμαστε τους δακτυλίους ΔΔΕ σαν τις κυκλικές ομάδες.
Το στοιχείο t θα το ονομάζουμε <u>ομοιομορφοποιητής</u> (<u>uniformizing parameter</u>) του R. Εύκολα παρατηρούμε ότι δεν υπάρχει μοναδικός ομοιομορφοποιητής και κάθε άλλος είναι της μορφής ut, u μονάδα.
Έστω K το σώμα κλασμάτων του R. Τότε για φιξαρισμένο ομοιομορφοποιητή t, κάθε μη μηδενικό στοιχείο $z \in K$ έχει μοναδική γραφή ως $z = ut^n, u$ μονάδα και $n \in \mathbb{Z}$ (τώρα παίρνει και αρνητικές τιμές). Ο εκθέτης n λέγεται τάξη του z και γράφεται $n = ord(z)$. Ορίζουμε $ord(0) = \infty$.
Απ΄ όλα τα προηγούμενα συμπεραίνουμε ότι $R = \{z \in K | ord(z) \geq 0\}$ και $M = \{z \in K | ord(z) > 0\}$.

Η συνάρτηση της τάξης ενός στοιχείου θα μας απασχολήσει και παρακάτω οπότε αξίζει να δώσουμε λίγη παραπάνω προσοχή.
Γενικά, η συνάρτηση τάξης είναι μία συνάρτηση που ορίζεται σε σώματα. Ας δώσουμε έναν πιο αυστηρό ορισμό.

Ορισμός 2.6. *Έστω K σώμα. Μία συνάρτηση $\phi : K \twoheadrightarrow \mathbb{Z} \cup \infty$ (επί) λέγεται <u>συνάρτηση τάξης</u> εάν ικανοποιεί τα παρακάτω:*

1. $\phi(a) = \infty \Leftrightarrow a = 0$.
2. $\phi(ab) = \phi(a) + \phi(b)$.
3. $\phi(a + b) \geq \min\{\phi(a), \phi(b)\}$.

Εύκολα παρατηρούμε ότι ο ορισμός αυτός συνδέεται με όσα έχουμε πει μέχρι τώρα. Μάλιστα η επόμενη πρόταση θα μας εξασφαλίσει ότι αυτή η συνάρτηση τάξης χαρακτηρίζει πλήρως έναν ΔΔΕ και αντίστροφα.

Πρόταση 2.13. *Αν $\phi : K \to Z \cup \infty$ μία συνάρτηση τάξης, τότε $R = \{z \in K | \phi(z) \geq 0\}$ είναι ΔΔΕ και $M = \{z | \phi(z) > 0\}$ το μέγιστο ιδεώδες και K το σώμα κλασμάτων.*
Αντίστροφα αν R είναι ΔΔΕ με σώμα κλασμάτων K, τότε η συνάρτηση $ord : K \to \mathbb{Z} \cup \infty$ είναι συνάρτηση τάξης. Το να δίνεται ένα ΔΔΕ με σώμα κλασμάτων K, λοιπόν, είναι ίδιο με το να ορίζεται μία συνάρτηση τάξης.

Απόδειξη. Θα χρησιμοποιήσουμε την προηγούμενη πρόταση και θα προσπαθήσουμε να δείξουμε ότι κάθε μη μηδενικό $z \in R$ γράφεται με μοναδικό τρόπο στη μορφή $z = ut^n$.
Έστω ϕ μία συνάρτηση τάξης και $R = \{z \in K | \phi(z) \geq 0\}$. Τότε $\phi(1_K) = \phi(1_K 1_K) = \phi(1_K) + \phi(1_K) \Rightarrow \phi(1_K) = 0$. Έστω $u \in R : \phi(u) = 0$, τότε $\phi(1_K)\phi(\frac{1}{u}u) = \phi(u) + \phi(\frac{1}{u}) = 0 \Rightarrow \phi(\frac{1}{u}) = 0 \Rightarrow \frac{1}{u} \in R$. Άρα αν $\phi(u) = 0 \Rightarrow u$ αντιστρέψιμο στο R.
Αφού ϕ επί άρα υπάρχει $t \in R : \phi(t) = 1$. Φιξάρουμε ένα τέτοιο t. Έστω $a, b \in R : \phi(a) = \phi(b)$. Θα δείξουμε ότι $b = ua$ όπου $\phi(u) = 0$. Πράγματι στο K μέσα το b μπορεί να γραφεί ως $b = za, z \in K, a, b \in R \Rightarrow \phi(b) = \phi(z) + \phi(a) \overset{\phi(a)=\phi(b)}{\Rightarrow} \phi(z) = 0 \Rightarrow z \in R$ και z αντιστρέψιμο. Το ανάποδο είναι προφανές. Συνεπώς $\phi(b) = \phi(a) \Leftrightarrow b = ua, u$ μονάδα στο R.
Έχουμε λοιπόν τις εξής περιπτώσεις:
Έστω $z \in R$. Εάν $\phi(z) = 0 \Rightarrow z = zt^0$
Εάν $\phi(z) = n > 0 \Rightarrow \phi(z) = \phi(t^n) \Rightarrow \exists u \in R$μονάδα $: z = ut^n$
Εάν $\phi(z) = \infty \Rightarrow z = 0$.
Δείξαμε λοιπόν ότι κάθε στοιχείο $z \in R$ μπορεί να γραφεί ως $z = ut^n, n \geq 0, u$ μονάδα. Για τη μοναδικότητα, έστω $ut^n = vt^m \Rightarrow \phi(ut^n) = \phi(vt^m) \Rightarrow n = m, u = v$. Συνεπώς από την προηγούμενη πρόταση, ο R είναι ΔΔΕ. Το μέγιστο ιδεώδες είναι $M = (t) = \{z \in R | \phi(z) \geq 0\}$.

Ανάποδα, έστω R ΔΔΕ με σώμα κλασμάτων K και $M = (t)$ το μέγιστο κύριο ιδεώδες.
Έστω $z \in K$, τότε $\exists!$μμονάδα $\in R, n \in \mathbb{Z} : z = ut^n$. Το ότι η $ord : K \to \mathbb{Z} \cup \infty$ είναι επί και ότι ισχύει η πρώτη ιδιότητα είναι προφανές. Έστω $a, b \in K \Rightarrow a = ut^n, b = vt^m \Rightarrow ord(ab) = ord(uvt^{n+m}) = n + m = ord(a) + ord(b)$ που δείχνει την δεύτερη ιδιότητα.
Έστω χ.β.γ ότι $min(n, m) = n$, τότε $ord(a + b) = ord(ut^n + vt^n t^{m-n}) = ord(t^n(u + vt^{m-n})) = n + ord(u + vt^{m-n})$. Αρκεί να δείξουμε ότι $ord(u + vt^{m-n}) \geq 0$. Από το δεύτερο κομμάτι της απόδειξης της προηγούμενης πρότασης έχουμε δείξει ότι $ord(u + vt^k, k \geq 0) = \begin{cases} 0 & \text{αν } u \neq 0 \\ k & \text{αν } \quad u = 0 \end{cases}$
Σε κάθε περίπτωση $ord(a + b) \geq ord(a) = n$. □

Μία χρήσιμη παρατήρηση που αξίζει να σημειωθεί και την οποία έχουμε συμπεράνει μέσα από τις δύο τελευταίες αποδείξεις είναι το εξής λήμμα.

Λήμμα 2.1. *Αν R ΔΔΕ και $u \in R$ μονάδα (μη μηδενική), τότε $u + vt^n$ είναι αντιστρέψιμο για κάθε $n \in N$ (δηλαδή $\phi(u + vt^n) = 0$*

Για την απόδειξη δείτε τις δύο παραπάνω αποδείξεις.

Η τάξη των στοιχείων κατά μία έννοια διαμερίζει το χώρο σε διαφορετικές κλάσεις, με κάθε κλάση να περιέχει στοιχεία μιας συγκεκριμένης τάξης. Θα δούμε ότι υπό μία έννοια, στοιχεία διαφορετικών τάξεων είναι γραμμικά ανεξάρτητα μεταξύ τους.

Πρόταση 2.14. *Έστω R ΔΔΕ με K σ.κ και ordτη συνάρτηση τάξης στο K.*

1. *Αν $ord(a) < ord(b)$, τότε $ord(a+b) = ord(a)$.*
2. *Αν $a_1, ..., a_n \in K$ και για κάποιο $i, ord(a_i) < ord(a_j) \forall j \neq i$, τότε $a_1 + ... + a_n \neq 0$.*

Απόδειξη. Η πρόταση αυτή δεν είναι παρά άμεση συνέπεια του παραπάνω λήμματος.
(1): Αν $a = ut^n, b = vt^m$ και $n < m$ τότε $ord(a+b) = ord(ut^n = vt^n t^{m-n}) = n + ord(u + vt^{n-m}) = n \overset{\text{λήμμα}}{=} ord(a)$.
(2): Με επαγωγή: Για $n = 2$, αν $ord(a_1) < ord(a_2) \Rightarrow ord(a_1 + a_2) \overset{(1)}{=} ord(a_1) \neq \infty \Rightarrow a_1 + a_2 \neq 0$.
Εάν ισχύει για n και $a_1, ..., a_n, a_{n+1} \in K$ τ.ω $ord(a_1) < ord(a_j) \forall j > 1$, τότε θέτοντας $b = a_1 + a_2$, έχουμε από το (1) ότι $ord(b) \overset{(1)}{=} < ord(a_j) \forall j > 2$ και άρα από υπόθεση επαγωγής $b + a_3 + ... + a_n \neq 0$ □

Οι προηγούμενες προτάσεις, παρόλο που είναι χρήσιμες κι από μόνες τους, τις χρειαζόμαστε κυρίως για να αποδείξουμε την επόμενη βασική πρόταση, που αν και αρχικά ίσως φαίνεται αρκετά τεχνική, θα αναδειχτεί η σημασία της στα επόμενα κεφάλαια.

Πρόταση 2.15. *Έστω R ΔΔΕ με μέγιστο ιδεώδες M και σ.κ K. Έστω ένα σώμα k υποδακτύλιο του R, δηλ $k \subset R$ και ότι η σύνθεση $k \to R \to R/M$ είναι ισομορφισμός του k με το R/M. Τότε ισχύουν τα ακόλουθα:*

1. *Για κάθε $z \in R$ υπάρχει μοναδικό $\lambda \in k : z - \lambda \in M$.*
2. *Έστω t ομοιομορφοποιητής του R και $z \in R$. Τότε για κάθε $n \geq 0$ υπάρχουν μοναδικά $\lambda_1, \lambda_1, ..., \lambda_n \in k$ και $z_n \in R$ τ.ω $z = \lambda_0 + \lambda_1 t + \lambda_2 t^2 + ... + \lambda_n t^n + z_n t^{n+1}$.*

Απόδειξη. 1. Έστω $z \in R$. Θυμίζουμε ότι το μέγιστο ιδεώδες σε ένα ΔΔΕ αποτελείται απ΄ όλα τα μη αντιστρέψιμα στοιχεία. Συνεπώς εάν z όχι αντιστρέψιμο, τότε για $\lambda = 0$ έχουμε τετριμμένα τελειώσει.
Έστω λοιπόν ότι z μονάδα στο R. Τότε η εικόνα του z στο R/M είναι $\bar{z} = z + M \neq 0_{R/M}$. Όμως, από υπόθεση $k \cong R/M$ και άρα $\exists \lambda \in k : \bar{\lambda} = \bar{z} = z + M \Rightarrow \bar{z} - \bar{\lambda} = 0_{R_M} \Rightarrow z - \lambda \in M$.
Μένει η μοναδικότητα. Έστω $\phi : k \to R/M, \phi(k) = k + M$. Αφού $R/M \cong k \Rightarrow ker(\phi) = 0_k$. Έστω $\lambda_1, \lambda_2 \in k : z - \lambda_1 \in M$ και $z - \lambda_2 \in M$. Τότε $z - \lambda_1 + M = z - \lambda_2 + M = 0 \Rightarrow (\lambda_1 - \lambda_2) + M = 0_{R/M} \Rightarrow \lambda_1 - \lambda \in ker(\phi) \Rightarrow \lambda_1 = \lambda_2$ και προκύπτει το ζητούμενο.

2. Το δεύτερο ερώτημα έχει περισσότερη δουλειά. Πρώτα θα δείξουμε την ύπαρξη, με επαγωγή στο n.
Για $n = 1$ έχουμε από το (1) ότι $\exists! \lambda_0 \in k : z - \lambda_0 \in M$. Όμως $M = (t)$ και άρα $z - \lambda_0 = ut^m$ για uμονάδα και $m \geq 1$. Εάν $m = 1$, έχουμε τελειώσει. Εάν $m > 1$ τότε $z - \lambda_0 = ut^m = (ut^{m-1})t \overset{z_0 = ut^{m-1}}{=} z_0 t$ που είναι στη μορφή που θέλουμε.
Έστω τώρα ότι ισχύει για n, δηλαδή για $z \in R, \exists \lambda_0, ..., \lambda_n \in k, z_n \in R : z = \lambda_0 + ... + \lambda_n t^n + z_{n+1} t^{n+1}$.
Τότε $z_{n+1} \in R \Rightarrow \exists! z_{n+2} \in \mathbb{R}, \lambda_{n+1} \in k : z_{n+1} = \lambda_{n+1} + z_{n+2} t$ (λόγω του (1». Αντικαθιστώντας στην παραπάνω εξίσωση έχουμε ότι $z = \lambda_0 + ... + \lambda_{n+1} t^{n+1} + z_{n+2} t^{n+2}$.

Μένει η μοναδικότητα την οποία θα δείξουμε μέσω της συνάρτησης τάξης, χρησιμοποιώντας και την προηγούμενη πρόταση ως βοηθό.

Έστω $z = \lambda_0 + ... + \lambda_n t^n + z_n t^{n+1} = m_0 + ... + m_n t^n + w_n t^{n+1}, w_n, z_n \in R, m_i, \lambda_i \in k$. Συνεπώς

$$(m_0 - \lambda_0) + (m_1 - \lambda_1)t + ... + (m_n - \lambda_n)t^n + (w_n - z_n)t^{n+1} = 0 \qquad (2)$$

Όμως $ord(m_i - \lambda_i) = 0 \forall i = 0, .., n$ αφού $m_i - \lambda_i \in k \subset R$ και άρα αντιστρέψιμα (και άρα η διαφορά τους αντιστρέψιμη).
Συνεπώς $ord(m_0 - \lambda_0) = 0, ord((m_1 - \lambda_1)t) = 1, ..., ord((m_n - \lambda_n)t^n) = n, ord((w_n - z_n)t^{n+1}) = (n+1) + ord(w_n - z_n) \geq n + 1$.

Συνεπώς η (2) είναι της μορφής $a_0+...+a_{n+1}=0$. Αν $a_0=m_0-\lambda_0\neq 0$ τότε $ord(a_0)=0<ord(a_j\forall j>0)$ και άρα από την προηγούμενη πρόταση $a_0+...+a_{n+1}\neq 0$ που είναι άτοπο. Αν $a_0=0$, τότε προχωράμε μέχρι το πρώτο i τ.ω $a_i\neq 0$. Τότε πάλι ισχύει το ίδιο επιχείρημα αφού $ord(a_i)<ord(a_j)\forall i\neq j$.

□

Πριν κλείσουμε αυτή την παράγραφο θα αναφέρουμε για εγκυκλοπαιδικούς λόγους την ετυμολογία του ¨Δακτύλιος διακριτής εκτίμησης' . Στην πραγματικότητα, υπάρχουν πολλοί ισοδύναμοι ορισμοί ενός ΔΔΕ. Ήδη εμείς είδαμε δύο από αυτούς. Ένας λοιπόν από τους ορισμούς αυτούς (τον οποίο δεν θα χρειαστούμε σε αυτά που μελετάμε) είναι ότι ένας υπόδακτύλιο R ενός σώματος κλασμάτων K λέγεται value ring εάν υπάρχει μια πλήρως διατεταγμένη αβελιανή ομάδα Γ (που ονομάζεται ομάδα εκτίμησης- value group -)και ένας επιμορφιμός ομάδων (που λέγεται εκτίμηση) $v:K^x\to\Gamma$ με $R=\{x\in K^x : v(x)\geq 0\}\cup\{0\}$. Ισοδύναμα, είναι μια ακεραία περιοχή R τ.ω για κάθε στοιχείο του x του σώματος κλασμάτων του F ισχύει ότι είτε $x\in R$ ή $x^{-1}\in R$. Η ομάδα εκτίμησης Γ λέγεται διακρητή (discrete) αν-ν η Γ είναι ισόμορφη με το $(\mathbb{Z},+)$. Τότε ο δακτύλιος P θα λέγεται ΔΔΕ. (για μια πιο προσεγμένη μελέτη των δακτυλίων εκτιμήσεων δείτε [Ηαρ] σελ.123).

2.3 Ευθέα γινόμενα Δακτυλίων

Οι δακτύλιοι που θα μελετήσουμε στα επόμενα κεφάλαια θα γράφονται ως γινόμενο δακτυλίων $X_{i=1}^n R_i$ στους οποίους θα χρειαστεί να υπολογίζουμε τη διάστασή τους. Σε αυτή την παράγραφο, λοιπόν, θα αναπτύξουμε την έννοια του γινομένου δακτυλίων και θα καταλήξουμε ότι η διάσταση όλου του χώρου ισούται με το άθροισμα των διαστάσεων των μικρότερων χώρων.

Έστω $R_1,...,R_n$ δακτύλιοι και $R_1\times...\times R_n$ το καρτεσιανό τους γινόμενο. Τότε αυτό φτιάχνεται σε δακτύλιο ορίζοντας την πρόσθεση ως $(a_1,...,a_n)+(b_1,...,b_n)=(a_1+b_1,...,a_n+b_n)$ και τον πολλαπλασιασμό επίσης κατά συντεταγμένη $(a_1,....,a_n)\cdot(b_1,...,b_n)=(a_1b_1,...,a_nb_n)$. Αυτός ο δακτύλιος λέγεται ευθύ γινόμενο του $R_1\times...\times R_n$ και συμβολίζεται με $X_{i=1}^n R_i$. Οι φυσικές προβολές $\pi_i : X_{j=1}^n\to R_i, \pi_i(a_1,...,a_n)=a_i$ εύκολα ελέγχουμε ότι είναι ομομορφισμοί δακτυλίων.

Το ευθύ γινόμενο χαρακτηρίζεται από την ακόλουθη ιδιότητα: Δοσμένου ενός δακτυλίου R και ενός ομομορφισμού δακτυλίων $\phi_i : R\to R_i, i=1,...,n$, υπάρχει μοναδικός ομομορφισμός $\phi : R\to X_{i=1}^n R_i$ τ.ω $\pi_i\circ\phi=\phi_i$ για κάθε i. Η απόδειξη είναι άμεση. Συγκεκριμένα, εάν ένα σώμα k είναι υποδακτύλιος κάθε R_i τότε το k μπορεί να θεωρηθεί ως υποδακτύλιος του $X_{i=1}^n R_i$.

Καταλήγουμε σε μια βασική πρόταση.

Πρόταση 2.16. *Εάν $k\subset R_i$ και κάθε R_i είναι πεπερασμένης διάστασης πάνω από το k τότε* $\dim(XR_i)=\sum\dim R_i$.

Απόδειξη. Έστω $n_i=\dim_k(R_i)$ και $B_1=\{a_1,...,a_{n1}\}$, ...,$B_i=\{\lambda_1,...,\lambda n_m\}$ βάση του κάθε R_i.
Θεωρούμε το σύνολο $B=\{(a_1,0,...,0),...,(a_{n1},0,...,0),...,(0,...,\lambda_1),...,(0,...,\lambda_{nm})\}$.Εύκολα βλέπουμε ότι το σύνολο αυτό έχει πλήθος nm στοιχεία και αποτελεί βάση του $X_{i=1}^m R_i$ (Η απόδειξη δεν παρουσιάζει καμιά δυσκολία, απλά είναι χρονοβόρα και παραλείπεται).

□

Η πρόταση αυτή θα παίξει καταλυτικό ρόλο στα επόμενα κεφάλαια και θα την επικαλούμαστε αρκετά συχνά.

2.4 Πράξεις με ιδεώδη

Για να προχωρήσουμε παρακάτω θα χρειαστούμε στο οπλοστάσιό μας αρκετά εργαλεία από την Αντιμεταθετική Άλγεβρα, όσον αφορά τις πράξεις με τα ιδεώδη. Τα καθαρά αλγεβρικά εργαλεία θα τα παρουσιάσουμε χωρίς αποδείξεις.

Έστω I, J ιδεώδη ενός δακτυλίου R. Θα θέλαμε ίσως να γράφαμε ως IJ το σύνολο $\{ab|a \in I, b \in J\}$. Εν γένει όμως το σύνολο αυτό δεν είναι από μόνο του ιδεώδες, οπότε ορίζουμε ως IJ το ιδεώδες που παράγεται από το $\{ab|a \in I, b \in J\}$. Όμοια, εάν $I_1, ..., I_n$ ιδεώδη, τότε ορίζουμε $I_1...I_n$ ως το ιδεώδες που παράγεται από το σύνολο $\{a_1....a_n|a_i \in I_i\}$. Ορίζουμε επιπλέον ως I^n το $I \cdot ... \cdot I$ (n φορές). Παρατηρείστε όμως ότι ενώ το I^n περιέχει όλες τις $n-$οστές δυνάμει των στοιχείων του I, δεν παράγεται αναγκαστικά από αυτές. Εάν το I παράγεται από τα $a_1, ..., a_r$ τότε το I^n παράγεται από τα $\{a_1^{i_1} \cdot ... \cdot a_r^{i_r} | \sum i_j = n\}$.

Παράδειγμα: Εάν $R = k[X_1, ..., X_r], I = (X_1, ..., X_r)$, τότε το I^n παράγεται από όλα το μονώνυμα βαθμού n και συνεπώς το I^n αποτελείται από όλα τα πολυώνυμα που κανένας τους όρος δεν έχει βαθμό $< n$. Συμπεραίνουμε, λοιπόν, ότι οι εικόνες των μονωνύμων βαθμού $< n$ δημιουργούν βάση του $k[X_1, ..., X_r]/I^n$ πάνω από το k.

Αν R υποδακτύλιος του δακτυλίου S και I ιδεώδες του R, τότε το IS συμβολίζει το ιδεώδες του S που παράγεται από το I. Εύκολα ελέγχουμε ότι $I^nS = (IS)^n$.

Έστω I, J ιδεώδη του R. Ορίζουμε $I + J = \{a + b|a \in I, b \in J\}$. Το $I + J$ είναι ιδεώδες και μάλιστα είναι το μικρότερο ιδεώδες που παράγεται από το $I/cupJ$(Θυμίζουμε ότι το $I \cup J$ δεν είναι εν γένει ιδεώδες).

Τα ιδεώδη I, J λέγονται μεταξύ τους μέγιστα εάν $I + J = R$, δηλαδή εάν $\exists a \in I, b \in J : 1 = a + b$.

Λήμμα 2.2. *1. $IJ \subset I \cap J$*

2. Αν I, J μεταξύ τους πρώτα, τότε $IJ = I \cap J$

Είναι καλό να έχουμε το παρακάτω σχήμα στο μυαλό μας για να διευκρινήσουμε τις σχέσεις εγκλεισμού.

$$\begin{tikzcd}
 & I+J \arrow[d, dash] & \\
 & I \cup J \arrow[dl, dash] \arrow[dr, dash] & \\
J \arrow[dr, dash] & & I \arrow[dl, dash] \\
 & I \cap J \arrow[d, dash] & \\
 & IJ &
\end{tikzcd}$$

Παρατήρηση: Κάνουμε την σύμβαση και θεωρούμε ότι ο R είναι υποδακτύλιος του S εάν πέρα από το να είναι ο ίδιος δακτύλιος, έχει επίσης και το ίδιο μοναδιαίο στοιχείο ($1_R = 1_S$). Αυτό εν γένει δεν ισχύει και μπορούμε να αντιπαραθέσουμε αρκετά παραδείγματα, τα οποία όμως δεν θα μας απασχολήσουν στην αλγεβρική γεωμετρία.

Τα επόμενα 4 λήμματα θα μας φανούν αρκετά χρήσιμα παρακάτω.

Πρόταση 2.17. *1. Έστω $I \subset J$ ιδεώδη στον R. Υπάρχει ένας φυσικός επιμομορφισμός από το R/I στο R/J*

2. Έστω I ιδεώδες του R και R υποδακτύλιος του δακτυλίου S. Υπάρχει ένας φυσικός ομομορφισμός από το R/I στο S/IS

Απόδειξη. (1) Θεωρούμε $\phi : R/I \to R/J, \phi(a + I) = a + J$. Αρκεί να δείξουμε ότι είναι καλά ορισμένος ομομορφισμός και επί.

Το ότι είναι ομομορφισμός είναι προφανές.
καλά ορισμένος: Έστω $a+I=b+I \Rightarrow a-b\in I$. Τότε $a-b\in I\subset J\Rightarrow a-b\in J$.
$\phi(a+I)=a+J, \phi(b+I)=b+J\Rightarrow \phi(a+I)=\phi(b+J)$ αφού $a-b+J=0$ Το επί είναι επίσης προφανές
(2) Θεωρούμε τον φυσικό ομομορφισμό $\pi: R\to S, \pi(a)=a$
και $\phi: R/I\to R/IS, \phi(a+I)=a+IS$.
Προφανώς ισχύει $\phi(a+I+b+I)=\phi(a+b+I)=a+b+IS=\phi(a+IS)+\phi(b+IS)$ και όμοια για τον πολλαπλασιασμό.
Εάν $a_1+I=a_2+I\Leftrightarrow a_1-a_2\in I\subset IS\Rightarrow a_1+IS=a_2+IS$ άρα καλά ορισμένος. □

Πρόταση 2.18. *Έστω I,J ιδεώδη του δακτυλίου R. Έστω I πεπερασμένα παραγόμενο και $I\subset\sqrt{J}$. Τότε υπάρχει $n\in\mathbb{N}$, τ.ω $I^n\subset J$.*

Απόδειξη. Έστω $I=(a_1,...,a_s)\subset J$. Άρα για κάθε $a_i, i=1,...,s$ υπάρχει ελάχιστος φυσικός n_i τ.ω $a_i^{n_i}\in J$. Έστω $N=max\{n_i\}$. Τότε $I^{Ns}\subset J$. Πράγματι, το I^{Ns} παράγεται από το σύνολο $A=\{a_1^{i_1}...a_s^{i_s}: i_1+...+i_s=Ns\}$.
Αν όλοι οι εκθέτες i_j είναι $i_j<N$ τότε $\sum i_j<Ns$ που είναι άτοπο. Άρα υπάρχει κάποιος εκθέτης $i_j: i_j\geq Ns\Rightarrow a_j^{i_j}\in J\Rightarrow a_1^{i_1}...a_s^{i_s}\in J\Rightarrow A\subset J$ Άρα $I^{Ns}\subset J$ □

Η παρακάτω πρόταση μοιάζει αρκετά περιορισμένη αλλά θα αποδειχτεί χρήσιμη.

Πρόταση 2.19. *Έστω $P=(0,...,0)\in A^n, \mathcal{O}=\mathcal{O}_P(A^n), M=M_P(A^n)$. Έστω $I=(X_1,...,X_n)\subset k[X_1,...,X_n]$. Τότε $I\mathcal{O}=M$ και άρα $I^r\mathcal{O}=M^r$ για κάθε r.*

Απόδειξη. Θέλουμε να δείξουμε ότι $I\mathcal{O}=M$. Παρατηρούμε ότι $\Gamma(A^n)=k[X_1,...,X_n], k(A^n)=k(X_1,..,X_n)$
Παρατηρούμε επίσης ότι $a\in I\Leftrightarrow a(0,...,0)=0$.
Έστω $f\in I\mathcal{O}\Rightarrow f=\sum a_ig_i, a_i\in I, g_i\in\mathcal{O}$
$=\sum a_i\frac{b_i}{c_i}, a_i\in I, b_i,c_i\in k[X_1,...,X_n], c_i(0,...0)\neq 0$. Συνεπώς $f(0,...,0)=0$ και άρα f όχι αντιστρέψιμο, άρα $f\in M\Rightarrow I\mathcal{O}\subset M$
Για τον αντίστροφο εγκλεισμό υποθέτουμε $g\in M\Rightarrow g=\frac{a}{b}, a,b\in k[X_1,...,X_n], a(0,...,0)=0, b(0,...,0)\neq 0$. Τότε $\frac{1}{b}\in\mathcal{O}, a\in I\Rightarrow a\cdot\frac{1}{b}=\frac{a}{b}\in I\mathcal{O}\Rightarrow M\subset I\mathcal{O}$. Συμπεραίνουμε ότι $I\mathcal{O}=M$ και άρα $I^r\mathcal{O}=(I\mathcal{O})^r=M^r$. □

Πρόταση 2.20. *Έστω V ποικιλότητα στο A^n ,$I=I(V)\subset k[X_1,...,X_n], P\in V$ και $J\supset I$ ιδεώδες του $k[X_1,...,X_n]$. Έστω J' η εικόνα του J στο $\Gamma(V)$. Τότε υπάρχει ένας φυσικός ομομορφισμός ϕ : $\mathcal{O}_P(A^n)/J\mathcal{O}_P(A^n)\to\mathcal{O}_P(V)/J'\mathcal{O}_P(V)$ και ότι ϕ ισομορφισμός.*
Συγκεκριμένα $\mathcal{O}_P(A^n)/I\mathcal{O}_P(A^n)\cong\mathcal{O}_P(V)$.
(Αυτό που θα χρειαστούμε εμείς είναι αυτό το τελευταίο αποτέλεσμα)

Απόδειξη. Έστω
$$\phi:\mathcal{O}_P(A^n)/J\mathcal{O}_P(A^n)\to\mathcal{O}_P(V)/J'\mathcal{O}_P(V)$$
,
$$\frac{a}{b}+J\mathcal{O}_P(A^n)\mapsto\frac{\bar{a}}{\bar{b}}+J\mathcal{O}_P(V)$$
όπου $\bar{a},\bar{b}$ οι εικόνες των a,b αντίστοιχα του φυσικού ομομορφισμού $\theta: k[X_1,...,X_n]\to k[X_1,...,X_n]/I, \theta(f)=f+I$. Παρατηρούμε ότι $J\mathcal{O}_P(A^n)=\{\sum a_i\frac{g_i}{h_i}, a_i\in J, g_i,h_i\in k[X_1,...,X_n], h_i(P)\neq 0\}$. Κάνοντας ¨ομώνυμα ' τα κλάσματα έχουμε ότι $f\in J\mathcal{O}_P(A^n)\Rightarrow f=\dfrac{\sum a_ig_i\prod_{j\neq i}h_j}{\prod h_i}$ και άρα βλέπουμε ότι είναι της μορφής (επειδή J ιδεώδες) : $f=\dfrac{g}{h}, g\in J, h\in k[X_1,...,X_n], h(P)\neq 0$.
Πολύ εύκολα ελέγχουμε ότι ο ϕ είναι καλά ορισμένος ομομορφισμός (όμοια όπως κάναμε στην πρόταση 2.15).

1-1 : Έστω $\phi(\frac{a}{b} + J\mathcal{O}_P(A^n)) = 0 + J\mathcal{O}_P(A^n))$
Συνεπώς $\frac{\overline{a}}{\overline{b}} \in J'\mathcal{O}_P(V)$. Αρκεί να δείξουμε ότι $\frac{a}{b} \in J\mathcal{O}_P(A^n)$, δηλαδή ότι $a \in J, b(P) \neq 0$. Όμως $J' = J + I(V)$ και $\mathcal{O}_P(V) = \{\sum \frac{c}{d}, c, d \in k[X_1, ..., X_n]/I(V), d(P) \neq 0\}$. Συμπεραίνουμε ότι $J'\mathcal{O}_P(V) = \{\sum e_i \frac{c_i}{d_i}, e_i \in J', c_i, d_i \in \Gamma(V), d_i(P) = 0\}$ και άρα είναι της μορφής $\{\frac{c}{d}, \quad c \in J', d \in \Gamma(V), d(P) \neq 0\}$.
Συνεπώς $\frac{\overline{a}}{\overline{b}} \in J'\mathcal{O}_P(V) \Rightarrow \overline{a} \in J', \overline{b}(P) \neq 0 \Rightarrow a \in J, b(P) \neq 0 \Rightarrow \frac{a}{b} \in J\mathcal{O}_P(A^n)$
Το ότι είναι επί είναι προφανές. Συνεπώς είναι ισομορφισμός, όπως θέλαμε. □

Συνδυάζοντας αυτή και την προηγούμενη παράγραφο καταλήγουμε σε ίσως την πιο σημαντική πρόταση του κεφαλαίου. Η απόδειξή της είναι αρκετά τεχνική, οπότε παραλείπεται.

Θεώρημα 2.1. *Έστω I ιδεώδες του $k[X_1, ..., X_n]$ (k αλγεβρικά κλειστό) και έστω $V(I) = \{P_1, ..., P_N\}$ πεπερασμένο. Έστω $\mathcal{O}_i = \mathcal{O}_{P_i}(A^n)$. Τότε υπάρχει ένας φυσικός ισομορφισμός του $k[X_1, ..., X_n]/I$ με το $X_{i=1}^n \mathcal{O}_i/I\mathcal{O}_i$.*

Άμεσα προκύπτουν δύο λήμματα.

Λήμμα 2.3. *Αν $V(I)$ πεπερασμένο, τότε $\dim_k(k[X_1, ..., X_n]/I) = \sum_{i=1}^n \dim_k(\mathcal{O}_i/I\mathcal{O}_i)$*

που είναι συνέπεια της πρότασης 2.16 και του παραπάνω θεωρήματος.

Λήμμα 2.4. *Αν $V(I) = \{P\}$, τότε $k[X_1, ..., X_n]/I \cong \mathcal{O}_P(A^n)/I\mathcal{O}_P(A^n)$*

2.5 R-modules και ακριβείς ακολουθίες

Πριν προχωρήσουμε στο επόμενο κεφάλαιο, χρειαζόμαστε τις έννοιες των R-module και των ακριβών ακολουθιών (exact sequences). Υπάρχει, φυσικά, πλούσια θεωρία πίσω από αυτές τις έννοιες αλλά για τις ανάγκες αυτής τις εργασίας δεν θα χρειαστούμε παρά τους ορισμούς και κάποια βασικά αποτελέσματα.

R-module Τα R-module είναι η γενίκευση των διανυσματικών χώρων. Θυμίζουμε ότι ο διανυσματικός χώρος είναι ένας χώρος πάνω από ένα σώμα k εφοδιασμένος με μία πράξη κι έναν βαθμωτό πολλαπλασιασμό που πληρούν κάποιες ιδιότητες. Όταν το k αυτό είναι απλά δακτύλιος και όχι αναγκαστικά σώμα τότε ο χώρος λέγεται R-module . Εάν το k είναι σώμα τότε οι έννοιες αυτές ταυτίζονται. Ας δώσουμε έναν πιο αυστηρό ορισμό.

Ορισμός 2.7. *Έστω R δακτύλιος. Ένα R-module είναι μία αντιμεταθετική ομάδα (με πράξη την ¨+' και ουδέτερο το 0_M) μαζί με έναν βαθμωτό πολλαπλασιασμό, δηλαδή μία συνάρτηση " $\cdot$ " : $R \times M \to M, (a, m) \mapsto a \cdot m$ που ικανοποιεί τα εξής:*

1. $(a + b)m = am + bm$ *για* $a, b \in R, m \in M$
2. $a \cdot (m + n) = am + an$ *για* $a \in R, m, n \in M$
3. $(ab) \cdot m = a \cdot (bm)$ *για* $a, b \in R, m \in M$
4. $1_R \cdot m = m$ *για* $m \in M$

Αμέσως προκύπτει ότι $0_R \cdot m = 0_M$ από την (1)
Μία υποομάδα N ενός $R - module$ M λέγεται submodule εάν για κάθε $a \in R, m \in N$ ισχύει ότι $am \in N$
Παρατηρήσεις: (α) Ένα $\mathbb{Z} - module$ δεν είναι παρά μια αντιμεταθετική ομάδα όπου $(\pm a)m = \pm(m + ... + m)$ (a φορές), για $a \in \mathbb{Z}, a \geq 0$
(β) Ο πολλαπλασιασμός στο R μετατρέπει κάθε ιδεώδες του σε R-module .
(γ) Αν $\phi : R \to S$ ομομορφισμός δακτυλίων τότε ορίζουμε $r \cdot s = \phi(r)s$. Αυτό μετατρέπει το S σε R-module . Γενικά, λοιπόν, εάν R υποδακτύλιος του S, τότε το S είναι R-module

Ακριβείς ακολουθίες Οι ακριβείς ακολουθίες όπως θα δούμε είναι ένα πολύ χρήσιμο εργαλείο για να μελετάμε διαστάσεις.

Έστω R δακτύλιος και M, M' R-modules . Ένας ομομορφισμός(αντ. ισομορφισμός) $\phi : M \to M'$ αβελιανών ομάδων λέγεται $R-module$ ομομορφισμός εάν $\phi(am) = a\phi(m)$.

Εάν N submodule ενός $R-module$ M τότε η ομάδα πηλίκο M/N μετατρέπεται σε $R-module$ με τον ακόλουθο τρόπο: εάν $\overline{m}$ η κλάση ισοδυναμίας του m και $a \in R$ ορίζουμε $a\bar{m} = \overline{am}$. Εύκολα ελέγχουμε ότι έτσι το M/N έχει μετατραπεί σε $R-module$. Το M/N λέγεται το module πηλίκο του M στο N.

Έστω $\psi : M' \to M, \phi : M \to M''$ να είναι $R-module$ ομομορφισμοί. Λέμε ότι η ακολουθία

$$M' \xrightarrow{\psi} M \xrightarrow{\phi} M''$$

είναι ακριβής εάν $Im(\psi) = ker(\phi)$. Παρατηρείστε ότι υπάρχει μοναδικός $R-module$ ομομορφισμός από το μηδενικό module 0 σε οποιοδήποτε $R-module$ M, όπως επίσης και από το M στο 0. Συνεπώς η ακολουθία $M \xrightarrow{\phi} M'' \longrightarrow 0$ είναι ακριβής αν-ν το ϕ είναι επί, ενώ η $0 \longrightarrow M' \xrightarrow{\psi} M$ είναι ακριβής αν-ν ψ είναι 1-1.
Εάν $\phi_i : M_i \to M_{i+1}$ είναι $R-module$ ομομορφισμοί τότε λέμε ότι η ακολουθία

$$M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} ... \xrightarrow{\phi_n} M_{n+1}$$

είναι ακριβής εάν $Im(\phi_i) = ker(\phi_1 i + 1)$ για κάθε $i = 1, ..., n$
Εμάς θα μας απασχολήσουν οι ακολουθίες που ξεκινάνε και τελειώνουν από και στο 0. Από τα παραπάνω συμπεραίνουμε ότι η ακολουθία $0 \longrightarrow M' \xrightarrow{\psi} M \xrightarrow{\phi} M'' \longleftrightarrow 0$ λέγεται ακριβής αν-ν η φ είναι επί, η ψ 1-1 και $Im(\psi) = ker(\phi)$. Οι ακριβείς ακολουθίες αυτής της μορφής λέγονται σύντομες ακριβείς ακολουθίες (short exact sequence).

Όπως αναφέραμε στην αρχή, οι ακριβείς ακολουθίες χρησιμεύουν στον υπολογισμό διαστάσεων, καθώς μεταφέρουν το πρόβλημα της διάστασης σε άλλους δακτυλίους που ίσως ο χειρισμός τους είναι πιο εύκολος. Ο τρόπος με τον οποίο γίνεται αυτό γίνεται ξεκάθαρος από την επόμενη πολύ σημαντική πρόταση.

Πρόταση 2.21. *(1): Έστω*

$$0 \longrightarrow V' \xrightarrow{\psi} V \xrightarrow{\phi} V'' \longrightarrow 0$$

μία σύντομη ακριβής ακολουθία πεπερασμένης διάστασης διανυσματικών χώρων πάνω από ένα σώμα k. Τότε $\dim V' + \dim V'' = \dim V$
(2) Έστω

$$0 \longrightarrow V_1 \xrightarrow{\phi_1} V_2 \xrightarrow{\phi_2} V_3 \xrightarrow{\phi_3} V_4 \longrightarrow 0$$

μία ακριβής ακολουθία πεπερασμένης διάστασης διανυσματικών χώρων. Τότε $\dim V_4 + \dim V_2 = \dim V_3 + \dim V_1$.

Απόδειξη. Το (1) είναι απλά μία αφηρημένη εκδοχή του θεωρήματος βαθμού μηδενικότητας από την γραμμική άλγεβρα για γραμμικούς μετασχηματισμούς $\phi : V \to V''$ πεπερασμένης διάστασης διανυσματικών χώρων.
Το (2) προκύπτει από το (1) ορίζοντας $W = Im(\phi_2) = ker(\phi_3)$. Πράγματι, οι ακολουθίες

$$0 \longrightarrow V_1 \xrightarrow{\phi_1} V_2 \xrightarrow{\phi_2} W \longrightarrow 0$$

και

$$0 \longrightarrow W \xrightarrow{\psi} V_3 \xrightarrow{\phi_3} V_4 \longrightarrow 0$$

είναι ακριβείς και ψ είναι εμφύτευση και άρα το αποτέλεσμα βγαίνει αφαιρώντας κατά μέλη. □

Το 2ο κομμάτι της απόδειξης δεν είναι παρά ένα επαγωγικό βήμα από $n = 3$ σε $n = 4$. Συνεχίζοντας με ακριβώς όμοιο τρόπο προκύπτει το επόμενο λήμμα

Λήμμα 2.5. *Έστω* $0 \longrightarrow V_1 \longrightarrow .... \longrightarrow V_n \longrightarrow 0$ *ακριβής ακολουθία πεπερασμένης διάστασης δ.χ. , τότε* $\sum(-1)^i \dim(V_i) = 0$.

Ακολουθούν δύο σημαντικές ασκήσεις/προτάσεις τις οποίες συχνά θα επικαλούμαστε στα επόμενα κεφάλαια.

Πρόταση 2.22. *(α) Έστω N submodule του M και π:M* $\to M/N$ *ο φυσικός ομομορφισμός. Έστω* $\phi : M \to M'$ *ένας ομομορφισμός των* $R-$ *modules και* $\phi(N) = 0$. *Τότε υπάρχει μοναδικός ομομορφισμός* $\overline{\phi} : M/N \to M'$ *τ.ω* $\overline{\phi} \circ \pi = \phi$.
(β) Αν N και P είναι submodules ενός module M, με $P \subset N$, *τότε υπάρχουν φυσικοί επιμομορφισμοί* $\phi_1 : N/P \to M/P$ *και* $\phi_2 : M/P \to M/N$. *Να δείξετε ότι η ακολουθία που προκύπτει*

$$0 \longrightarrow N/P \xrightarrow{\phi_1} M/P \xrightarrow{\phi_2} M/N \longrightarrow 0$$

είναι ακριβής (δεύτερο Θεώρημα Ισομορφίας της Noether).
(γ) Έστω $U \subset W \subset V$ *δ.χ με* V/U *πεπερασμένης διάστασης. Τότε* $\dim V/U = \dim V/W + \dim W/U$
(δ): Αν $I \subset J$ *ιδεώδη δακτυλίου R τότε υπάρχει μοναδική ακριβής ακολουθία από* $R-$ *modules:*

$$0 \longrightarrow I/J \longrightarrow R/J \longrightarrow R/I \longrightarrow 0$$

(ε) Αν $\mathcal{O}$ *τοπικός δακτύλιος με M το μέγιστο ιδεώδες, τότε υπάρχει μία φυσική ακριβής ακολουθία από* $\mathcal{O}-$ *modules :*

$$0 \longrightarrow M^n/M^{n+1} \longrightarrow \mathcal{O}/M^{n+1} \longrightarrow \mathcal{O}/M^n \longrightarrow 0$$

.

Απόδειξη. (α): Θεωρούμε $\bar{\phi} : M/N \to M', \bar{\phi}(\bar{m}) = \bar{\phi}(m+N) := \phi(m)$.
<u>Καλά ορισμένος:</u>
Έστω $m_1 + N = m_2 + n \Rightarrow m_1 - m_2 \in N$
$\bar{\phi}(m_1+N) - \bar{\phi}(m_2+N) = \phi(m_1) - \phi(m_2) \overset{\phi \text{ομομ.}}{=} \phi(m_1 - m_2) \overset{m_1-m_2 \in N}{=} 0 \Rightarrow \phi(m_1) = \phi(m_2)$.
Το ότι είναι ομομορφισμός είναι αρκετά προφανές, αφού φ ομομορφισμός.
Επιπλέον $\bar{\phi}(\pi(m)) = \bar{\phi}(m+n) = \phi(m)$ και άρα όντως $\phi = \bar{\phi} \circ \pi$
<u>Μοναδικότητα</u>
Έστω $\psi : M/N \to M'$ ένας $R-$ *module* ομομορφισμός και έστω $\psi \circ \pi = \phi = \bar{\phi} \circ \pi$. Όμως π επί. Άρα αν $\bar{m} \in M/N$ τότε $\psi(\bar{m}) = \psi(\pi(m)) = \bar{\phi}(\pi(m)) = \bar{\phi}(\bar{m})$. Άρα $\psi = \bar{\phi}$.

(β) Έστω $\phi_1 : N/P \to M+P$ και $\phi_2 : M/P \to M/N$.
$n+P \mapsto n+P \qquad m+P \mapsto m+N$
Το ότι η ϕ_1 είναι 1-1 και η ϕ_2 επί είναι προφανές. Μένει λοιπόν να δείξουμε ότι $Im(\phi_1) = kerf(\phi_2)$.
Πράγματι $m+P \in ker(\phi_2) \Leftrightarrow m \in N \Leftrightarrow \exists n \in N : \phi(n+P) = m+P \Leftrightarrow m+P \in Im(\phi_1)$ άρα όντως $Im(\phi_1) = ker(\phi_2)$
Συνεπώς η ακολουθία

$$0 \longrightarrow N/P \xrightarrow{\phi_1} M/P \xrightarrow{\phi_2} M/N \longrightarrow 0$$

είναι ακριβής
(γ) Έστω $U \subset W \subset V$ δ.χ και V/U πεπερασμένης διάστασης. Τα σύνολα $W/U, V/U, V/W$ είναι διανυσματικοί χώροι.
Αφού $W/U \subset V/U$ άρα $\dim(W/U) \leq \dim(V/U) = N < \infty$.
Θέλουμε να δείξουμε ότι $\dim(V/W) < \infty$.
Πράγματι εάν $B_1 = \{v_1+U, ..., v_N+U\}$ βάση του V/U τότε το σύνολο $B_2 = \{v_1+W, ..., v_N+W\}$ παράγει το V/W (όχι όμως αναγκαστικά βάση) και άρα $\dim(V/W) \leq \dim(V/U) < \infty$ (η επαλήθευση ότι το B_2 παράγει

τον χώρο είναι άμεση).
Από το (β) λοιπόν έχουμε ότι η ακολουθία

$$0 \longrightarrow W/U \longrightarrow V/U \longrightarrow V/W \longrightarrow 0$$

είναι ακριβής και όλα είναι δ.χ πεπερασμένης διάστασης και άρα από πρόταση 2.21 έχουμε $\dim(V/U) = \dim(W/U) + \dim(V/W)$ όπως θέλαμε.
(δ) Έστω $J \subset I$ ιδεώδη του R. Θυμίζουμε ότι ο πολλαπλασιασμός στο R μετατρέπει τα J, I σε $R-modules$. Συνεπώς τα $I/J, R/J, R/I$ είναι και αυτά $R-modules$. Το J μάλιστα είναι submodule του module I αφού για κάθε $a \in R, j \in J$ έχουμε ότι $a \cdot j \in J$ αφού J ιδεώδες. Το R είναι $R-module$ του εαυτού του. Από το (β) λοιπόν, θέτοντας $N = J, P = I, M = R$ έχουμε ότι η ακολουθία $0 \longrightarrow I/J \longrightarrow R/J \longrightarrow R/I \longrightarrow 0$ είναι ακριβής.

(ε) Θεωρούμε $R = \mathcal{O}, I = M^n, J = M^{n+1}$. Έχουμε ότι $J \subset I$ και I, J ιδεώδη και άρα από το (δ) προκύπτει το ζητούμενο. □

Η επόμενη πρόταση θα αποτελέσει συνδετικό κρίκο για ένα σημαντικό αποτέλεσμα του επόμενου κεφαλαίου. Για να την αποδείξουμε θα χρειαστούμε την Πρόταση 2.15.

Πρόταση 2.23. *Έστω R ένας ΔΔΕ που ικανοποιεί τις συνθήκες της πρότασης 2.15. Το M^n/M^{n+1} είναι $R-module$ και συνεπώς $k-module$ αφού $k \subset R$.*

1. *Ισχύει:* $\dim_k(M^n/M^{n+1}) = 1 \quad \forall n \geq 0$.
2. *Ισχύει:* $\dim_k(R/M^n) = n \quad \forall n \geq 0$
3. *Έστω $z \in R$. Τότε $ord(z) = n$ αν $(z) = M^n$ και συνεπώς $ord(z) = \dim_k(R/(z))$.*

Απόδειξη. 1. Έστω t ο ομοιομορφοποιητής του R. Τότε $M = (t), M^n = (t^n), M^{n+1} = (t^{n+1})$.
Έστω $z \in M^n/M^{n+1} \Rightarrow z = ut^n + M^{n+1}$.
Αν u όχι αντιστρέψιμο, τότε $u = u_0 t^m, u_0$ μονάδα και $m \geq 1$ και άρα $z = 0$. Συνεπώς, αν $z \neq 0 \Rightarrow u$ μονάδα, $z = ut^n + M^{n+1}$. $\Rightarrow\Rightarrow$ (1)
Από την πρ. 2.15, $\exists! \lambda \in k : u - \lambda \in M \Rightarrow u - \lambda = at^m, a$ μονάδα και $m \geq 1$. Συνεπώς $u = \lambda + at^m$. Αντικαθιστώντας στην (1) έχουμε ότι $z = \lambda t^n + M^{n+1}, \lambda \in k$. Άρα το $\{t^n + M^{n+1}\}$ είναι $k-$ βάση του $M^n/M^{n+1} \Rightarrow M^n/M^{n+1} \cong k$ και $\dim_k(M^n/M^{n+1}) = 1 \forall n \geq 1$
Για $n = 0$ έχουμε από υπόθεση ότι $R/M \cong k$.
2. Από το (β) της πρ. 2.15 έχουμε ότι $\forall z \in R, n \geq 0 \exists! \lambda_0, ..., \lambda_n \in k, z_n \in R$ τ.ω $z = \lambda_0 + \lambda_1 t + ... + \lambda_n t^n + z_n t^{n+1}$. Συνεπώς η εικόνα του z στο R/M^{n+1} είναι $\bar{z} = (\lambda_0 + M^{n+1}) + ... + (\lambda_n t^n + M^{n+1}$.
Άρα $R/M^n \cong X_{i=0}^{n-1} M^i/M^{i+1}$ και από της πρόταση 24 έχουμε ότι $\dim(X_{i=0}^{n-1} M^i/M^{i+1}) = \sum_{i=0}^{n-1} M^i/M^{i+1} = n$
3. Έστω $(z) = M^n = (t^n)$.
$z \in R \Rightarrow \exists u$ μονάδα και $m \in \mathbb{N} : z = ut^m$. Συνεπώς $(z) = (ut^m) = (t^m) = M^m = (t^n) = M^n \Leftrightarrow m = n($ η μία συνεπαγωγή είναι προφανής, η άλλη προκύπτει από το παρατηρώντας ότι εάν $m \leq n$ τότε το t^m δεν μπορεί να γραφεί ως $t^m = ut^n$ (γιατί; ». Άρα $ord(z) = n \overset{(2)}{=} \dim_k(R/(z)) = \dim_k(R/M^n)$.

□

Κεφάλαιο 3

Επίπεδες καμπύλες στον Αφφινικό χώρο

Στα πρώτα δύο κεφάλαια αναπτύξαμε όλη τα βασικά εργαλεία και τις βασικές γνώσεις που θα χρειαστούμε και τώρα επιτέλους είμαστε έτοιμοι να μπούμε στο κύριο αντικείμενο αυτής της εργασίας που είναι η μελέτη των επίπεδων καμπύλων στον χώρο. Αυτό που μας ενδιαφέρει περισσότερο είναι η μελέτη στον προβολικό χώρο για λόγους που αναπτύξαμε στην εισαγωγή αλλά για να το επιτύχουμε αυτό πρέπει πρώτα να μελετήσουμε τον αφφινικό.

Έχουμε δει ότι τις αφφινικές επίπεδες καμπύλες μπορούμε να τις παριστάνουμε με μη σταθερά πολυώνυμα $F \in k[X,Y]$ χωρίς πολλαπλούς παράγοντες. Πολλαπλασιάζοντας την καμπύλη επί μια σταθερά επίσης δεν αλλάζει τίποτα στο σχήμα , δηλαδή οι καμπύλες $F, \lambda F, \lambda \neq 0, \lambda \in k$ παριστούν την ίδια καμπύλη και συνεπώς θα τις ταυτίζουμε. Γενικά, λοιπόν θα λέμε ότι δύο πολυώνυμα $F, G \in k[X,Y]$ είναι ισοδύναμα, εάν υπάρχει μη μηδενικό $\lambda \in k : F = \lambda G$ και ορίζουμε μία αφφινική επίπεδη καμπύλη να είναι μία κλάση ισοδυναμίας μη σταθερών πολυωνύμων που συνδέονται με τη σχέση αυτής της ισοδυναμίας. Παρόλο που γεωμετρικά το σχήμα είναι το ίδιο, για λόγους που θα αναπτύξουμε στη συνέχεια, θα επιτρέπουμε την F να έχει πολλαπλούς παράγοντες και άρα η καμπύλη $F = X$ είναι διαφορετική από την $F = X^2$.

Συχνά κάνουμε την παρατυπία και συγχέουμε την καμπύλη με το πολυώνυμο, και θα λέμε για παράδειγμα ¨η επίπεδη καμπύλη $Y^2 - X^3$' ή ' η επίπεδη καμπύλη $Y^2 = X^3$. Ο <u>βαθμός</u> μιας καμπύλης είναι ο βαθμος του πολυωνύμου που την ορίζει. Μία καμπύλη βαθμού 1 είναι ευθεία και άρα μιλάμε για την ¨ευθεία $aX + bY + c$ ή αλλιώς την ¨ευθεία $aX + bY + c = 0$.

Η μελέτη των καμπυλών λοιπόν θα γίνει μέσω της μελέτης των πολυωνύμων $F \in k[X,Y]$. Για την καλύτερη μελέτη θα χρειαστεί να χωρίζουμε το πολυώνυμο σε <u>ομογενείς</u> παράγοντες. Ένα πολυώνυμο λέγεται <u>ομογενές</u> ή <u>form</u> βαθμού d εάν αποτελείται μόνο από μονώνυμα <u>βαθμού</u> d. Κάθε πολύνυμο βαθμού n μπορεί να γραφεί με μοναδικό τρόπο ως άθροισμα $F = F_0 + F_1 + ... + F_n$ όπου F_i είναι ομογενές βαθμού i. Για παράδειγμα το $F = Y^2 - X^3$ είναι βαθμού 3, της μορφής $F = F_2 + F_3, F_2 = Y^2, F_3 = -X^3$. Θα χρησιμοποιήσουμε ως γεγονός ότι κάθε ομογενές πολυώνυμο $F \in k[X,Y]$ μπορεί να παραγαντοποιηθεί k (αλγεβρικά κλειστό) σε γινόμενο γραμμικών παραγόντων δηλαδή $F = \prod F_i^{e_i}, \deg(F_i) = 1$ Παρατηρείστε ότι αυτό δεν συμβαίνει εάν F όχι ομογενές ή αν είμαστε στο $k[X_1, ..., X_n], n \geq 3$.

Γενικά όμως ένα πολυώνυμο $F \in k[X,Y]$ μπορούμε να το παραγοντοποιούμε σε ανάγωγους παράγοντες $F = \prod F_i^{e_i}, F_i$ ανάγωγα. Λέμε ότι τα F_i είναι οι παράγοντες του F και ότι το e_i είναι η πολλαπλότητα του παράγοντα F_i. Εάν $e_i = 1$ λέμε ότι ο παράγοντας F_i είναι απλός, αλλιώς λέμε ότι είναι πολλαπλός.
Παρατηρείστε ότι εάν γνωρίζουμε μόνο την γεωμετρική εικόνα, δηλαδή το $V(F)$ μπορούμε να βρούμε τους παράγοντες F_i αλλά όχι την πολλαπλότητά τους. Για παράδειγμα το $F = X^2$ γεωμετρικά παριστά τον άξονα τον ψ, $V(F) = \{(0,y), y \in k\}$. Εάν δεν γνωρίζουμε το F, τότε από το $V(F)$ μπορούμε να βρούμε το $I(V(F)) = X = \sqrt{F}$. Βρήκαμε δηλαδή τον παράγοντα του F αλλά όχι την πολλαπλότητά του. Ο λόγος είναι το Nullstellensats που μας λέει ότι $I(V(F)) = \sqrt{F}$.

Εάν το F είναι ανάγωγο, το $V(F)$ είναι ποικιλότητα. Συνήθως γράφουμε $\Gamma(F), k(F)$, και $\mathcal{O}_P(F)$ αντί για

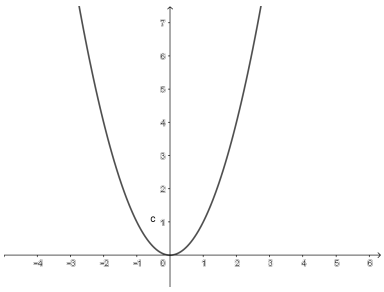
$\Gamma(V(F)), k(V(F)), \mathcal{O}_P(V(F))$.

3.1 Πολλαπλά σημεία και Εφαπτόμενες Ευθείες

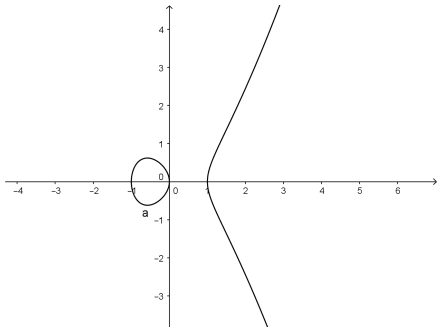
Έστω F καμπύλη και $P = (a, b) \in F$. Το P λέγεται απλό σημείο της F εάν δεν μηδενίζει κάποια παράγωγό της, δηλαδή $F_X(P) \neq 0$ ή $F_Y(P) \neq 0$. Σε αυτή την περίπτωση, η ευθεία $F_X(P)(X-a)+F_Y(P)(Y-b) = 0$ λέγεται εφαπτόμετνη ευθεία της F στο P. Ένα σημείο που δεν είναι απλό, λέγεται πολλαπλό (ή ιδιάζον (singular ». Μία καμπύλη με μόνο απλά σημεία λέγεται μη χαρακτηριστική/μη ιδιάζουσα καμπύλη (non-singular curve)

Κάναμε ήδη την παρατήρηση στην παράγραφο Noetherina Decomposition αλλά ξανατονίζουμε ότι τα σχήματα που βλέπουμε γεωμετρικά παριστούν μόνο το πραγματικό κομμάτι της καμπύλης, δηλαδή το $F \cap A^2(\mathbb{R})$. Παρόλο που οι εικόνες είναι χρήσιμες στην καλύτερη κατανόηση δεν πρέπει να βασιζόμαστε αποκλειστικά πάνω σε αυτές.

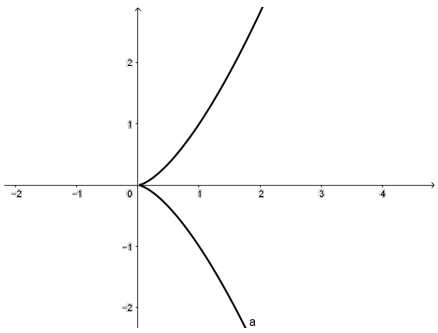
Παραδείγματα:



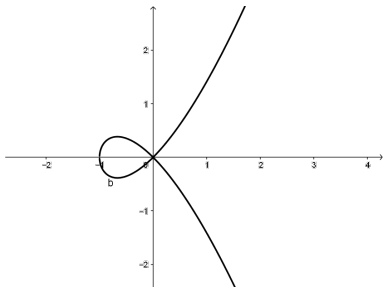
Σχήμα 3.1: $A = Y - X^2$



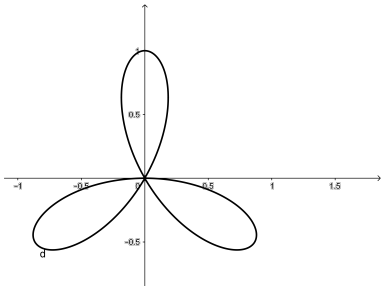
Σχήμα 3.2: $B = Y^2 - X^3 + X$



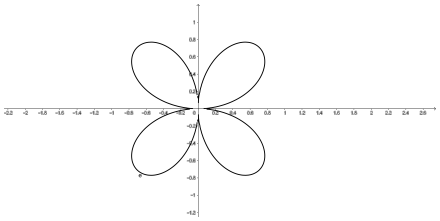
Σχήμα 3.3: $C = Y^2 - X^3$



Σχήμα 3.4: $D = Y^2 - X^3 - X^2$



Σχήμα 3.5: $E = (X^2 + Y^2)^2 + 3X^2Y - Y^3$



Σχήμα 3.6: $F = (X^2 + Y^2)^3 - 4X^2Y^2$

Με απλούς υπολογισμούς με τις παραγώγους τους, βλέπουμε ότι τα πρώτα δύο σχήματα (3.1 3.2) είναι μη χαρακτηριστικές δηλαδή όλα τους τα σημεία είναι απλά.

Στις C, D, E, F το μόνο πολλαπλό σημείο είναι το $P = (0, 0)$

Παρατηρείστε ότι στα πρώτα δύο παραδείγματα ο γραμμικός όρος των εξισώσεων των καμπυλών είναι απλά η εφαπτόμενη τους στο σημείο $P = (0, 0)$, ενώ στις υπόλοιπες καμπύλες, το χαμηλότερο ομογενές πολύνυμο των εξισώσεων (Y^2 για την C, $Y^2 - X^2 = (Y - X)(Y + X)$ για την D, $3X^2Y - Y^3 = Y(\sqrt{r}X - Y)(\sqrt{3}X + Y)$ για την E, $-4X^2Y^2$ για την F) αποτελούν τις ευθείες που καλύτερα μπορούν να χαρακτηρισθούν ως εφαπτόμενες των καμπυλών στο $(0, 0)$. Όπως θα δούμε το γεγονός αυτό δεν είναι καθόλου τυχαίο και με λίγη εξάσκηση με το ¨μάτι' και μόνο θα είναι κανείς σε θέση να καταλαβαίνει την πολλαπλότητα ενός σημείου μιας καμπύλης. Διαισθητικά και μόνο αναφέρουμε ότι στο A ο άξονας τον X εφάπτεται εξολοκλήρου και με ¨ομαλό' τρόπο στην καμπύληκαι ως εκ τούτου το σημείο $(0, 0)$ είναι απλό σημείο, ενώ στην C ο άξονας των X εφάπτεται με ¨διαφορετικό τρόπο' στον πάνω και στο κάτω μέρος της καμπύλης (θα δούμε στη συνέχεια ότι το σημείο αυτό λέγεται αιχμηρό (cusp)), είναι δηλαδή διπλή εφαπτομένη. Αντίστοιχα στην E βλέπουμε ότι στο $(0, 0)$ μπορούμε να θεωρήσουμε 3 διαφορετικές ¨εφαπτομένες' ευθείες, αυτές που προκύπτουν από την παραγοντοποίηση του μικρότερου ομογενούς πολυωνύμου και άρα θα πούμε ότι το σημείο έχει πολλαπλότητα 3, ενώ στην F θα έχει πολλαπλότητα 4 κ.ο.κ. Η διαίσθησή μας χάνεται σε παραδείγματα όπως το B (ανατρέξτε στο αντίστοιχο σχήμα στην παράγραφο της ανάλυσης της Noether 1.8)

Ας τα εξηγήσουμε όμως πιο αυστηρά. Όλη μας την μελέτη θα την κάνουμε γύρω από το σημείο $P = (0, 0)$ κι έπειτα θα τη γενικεύσουμε. Έστω F μία καμπύλη και $P = (0, 0)$. Γράφουμε την F ως $F = F_m + F_{m+1} + ... + F_n$ όπου F_i ομογενές βαθμού i και $F_m \neq 0$. Ορίζουμε το m να είναι η πολλαπλότητα της F στο σημείο $P = (0, 0)$ και γράφουμε $m = m_P(F)$. Παρατηρείστε ότι $P \in F \Leftrightarrow m_P(F) > 0$. Χρησιμοποιώντας τον κανόνα με τις παραγώγους που αναφέραμε προηγουμένως αμέσως βλέπουμε ότι το P είναι απλό αν-ν $m_P(F) = 1$ και σε αυτή την περίπτωση η F_1 είναι ακριβώς η εφαπτόμενη της F στο P. Αν $m = 2$ τότε το P λέγεται διπλό σημείο και αν $m = 3$ τριπλό κτλ.

Αφού το F_m είναι ομογενές σε 2 μεταβλητές, μπορούμε να το παραγοντοποιήσουμε σε γραμμικούς παράγοντες $F_m = \prod L_i^{r_i}$, όπου L_i διακεκριμένες ευθείες. Οι L_i λέγονται εφαπτόμενες ευθείες της F στο $P = (0, 0)$ και r_i είναι η πολλαπλότητα κάθε εφαπτομένης. Η L_i λέγεται απλή (αντ. διπλή κτλ) εάν $r_i = 1$ (αντ 2 κτλ). Εάν η F έχει m διακεκριμένες (απλές) εφαπτόμενες ευθείες στο P τότε το P λέγεται σύνηθες πολλαπλό σημείο(ordinary multiple point) της F (Εάν έχει m διακεκριμένες εφαπτόμενες τότε αναγκαστικά είναι απλές). Ένα σύνηθες διπλό σημείο λέγεται κόμβος (node). (Η D έχει κόμβο στο $P = (0, 0)$, η F έχει σύνηθες τριπλό σημείο ενώ η C και E έχουν μη-σύνηθες πολλαπλό σημείο στο $(0, 0)$.) Για ευκολία μία ευθεία που περνάει από το P αλλά δεν είναι εφαπτόμενη της F την χαρακτηρίζουμε ως εφαπτόμενη πολλαπλότητας 0.

Έστω $F = \prod F_i^{e_i}$ η παραγοντοποίηση της Fσε ανάγωγους παράγοντες. Τότε $m_P(F) = \sum e_i m_p(F_i)$. Εάν L εφαπτόμενη ευθεία του F_i με πολλαπλότητα r_i τότε η L είναι εφαπτόμενη στην F με πολλαπλότητα $\sum e_i r_i$. (Αυτό είναι συνέπεια του γεγονότος ότι το το ομογενές με το μικρότερο βαθμό στην F προκύπτει από το γινόμενο των ομογενών πολυωνύμων με τον μικρότερο βαθμό των παραγόντων της.)

Συγκεκριμένα ένα σημείο P λέγεται απλό της F αν-ν το P ανήκει μόνο σε έναν παράγοντα F_i της F, όπου

F_i απλός παράγοντας και P απλό σημείο στην F_i.

Για να επεκτείνουμε τους ορισμούς που εισάγαμε μέχρι τώρα για ένα τυχαίο σημείο $P = (a, b) \neq (0, 0)$ χρησιμοποιούμε μία μετατόπιση/αλλαγή συντεταγμένων που στέλνει το $(0, 0)$ στο (a, b), δηλαδή την $T(X, Y) = (X + a, Y + b)$. Τότε $F^T = F(X + a, Y + b)$. ορίζουμε $m_P(F) := m_{(0,0)}(F^T)$. Δηλαδή εάν γράψουμε την F^T ως $F^T = G_m + ...$, G_i ομογενή τότε $m_P(F) = m_{(0,0)}(F^T) = m$. Όλοι οι υπόλοιποι ορισμοί (εφαπτόμενη ευθεία, πολλαπλότητα σημείου κ.τ.λ) επεκτείνονται με τον ίδιο τρόπο. Παρατηρείστε ότι η μετατόπιση αυτή στέλνει σημεία του F^T σε σημεία της F και τις εφαπτόμενες της F^T στο $(0, 0)$ στις εφαπτόμενες της F στο P.

Περιληπτικά τα όσα είπαμε συμπικνώνονται στον παρακάτω πίνακα

Αν $F = F_m + ... + F_n$, τότε $m_P(F) = m$

• Αν $m = 0 \Rightarrow P \notin F$

Αν $m = 1 \Rightarrow P$ απλό σημείο

Αν $m > 1 \Rightarrow P$ πολλαπλό

$F_m = \prod L_i^{e_i}$

• Αν $e_i = 1$για κάθε i, τότε $Pordinary$ και L_i απλή εφαπτομένη

Αν $e_i = 2 \longrightarrow L_i$ διπλή εφαπτομένη.

Αν $m_P(F) = 2$ και P απλό, τότε P node

Αν $P = (a, b) \neq (0, 0)$, τότε $T = (X + a, Y + b)translation$ και θεωρούμε F^T

Οι ορισμοί που δώσαμε εν μέρει γενικεύονται και σε υπερεπιφάνειες στον $k[X_1, ..., X_n]$ αλλά συναντάμε κάποια προβλήματα. Όπως πριν γράφουμε την F ως $F = F_m + ... + F_n$ και ορίζουμε $m_{(0,0)}(F) = m$ και για $P = (a_1, ..., a_n)$ χρησιμοποιούμε πάλι την $T = (X_1 + a_1, ...X_n + a_n)$ και ορίζουμε $m_P(F) := m_{(0,0)}(F^T)$. Εάν $m_P(F) = 1$ αντί για εφαπτόμενη ευθεία θα έχουμε τώρα εφαπτόμενο υπερεπίπεδο, το οποίο θα είναι το

$$F_{X_1}(P)(X_1 - a_1) + ... + F_{X_n}(P)(X_n - a_n)\text{για } P = (0, ..., 0)$$

$$F^T_{X_1}(P)(X_1 - a_1) + ... + F^T_{X_n}(P)(X_n - a_n)\text{για } P = (a_1, ..., a_n)$$

Παρόλαυτά δεν μπορούμε να χαρακτηρίσουμε τα υπερεπίπεδα στα πολλαπλά σημεία. Ο λόγος είναι ότι δεν μπορούμε πάντα να αναλύσουμε ένα ομογενές πολυώνυμο μεγαλύτερων διαστάσεων σε γινόμενο υπερεπιπέδων. Για παράδειγμα θα δούμε την υπερεπιφάνεια $F = X^2 + Y^2 - Z^2$, $P = (0, 0, 0)$.Παρατηρούμε ότι είναι ήδη ομογενές. Αν παραγοντοποιείται σε γινόμενο υπερεπιπέδων τότε θα είναι της μορφής

$F = X^2 + Y^2 + Z^2 = (a_1X + a_2Y + a_3Z)(b_1X + b_2Y + b_3Z) = a_1b_1X^2 + a_2b_2Y^2 + a_3b_3Z^2 + a_1b_2XY + a_1b_3XZ + a_2b_1XY + a_2b_3YZ + a_3b_1XZ + a_3b_2YZ$

Παίρνουμε λοιπόν το σύστημα

$$\begin{cases} a_1b_1 = 1 \\ a_2b_2 = 1 \\ a_3b_3 = -1 \\ a_1b_2 + a_2b_1 = 0 \Rightarrow \frac{b_2}{b_1} + \frac{b_1}{b_2} = 0 \Rightarrow b_1^2 + b_2^2 = 0 \\ a_1b_3 + a_3b_1 = 0 \Rightarrow \frac{b_3}{b_1} - \frac{b_1}{b_3} = 0 \Rightarrow b_3^2 - b_1^2 = 0 \\ a_2b_3 + a_3b_2 = 0 \Rightarrow \frac{b_3}{b_2} - \frac{b_2}{b_3} = 0 \Rightarrow b_3^2 - b_2^2 = 0 \end{cases}$$

Από τις 2 τελευταίες παίρνουμε ότι $b_2^2 = b_1^2$ και από την 3η από το τέλο συμπεραίνουμε ότι $b_1 = b_2 = b_3 = 0$ που είναι άτοπο. Άρα δεν μπορεί να παραγοντοποιηθεί.

Μία άλλη ειδοποιός διαφορά είναι στο πλήθος των πολλαπλών σημείων. Ισχύει η παρακάτω πρόταση.

Πρόταση 3.1. *Μία ανάγωγη επίπεδη καμπύλη έχει μόνο πεπερασμένο αριθμό από πολλαπλά σημεία. Δεν ισχύει το ίδιο για υπερεπιφάνειες.*

Απόδειξη. Θα χρησιμοποιήσουμε τον πρώτο ορισμό που δώσαμε για τα πολλαπλά σημεία. P πολλαπλό αν-ν $F_X(P) = F_Y(P) = 0 = F(P) \Leftrightarrow P \in V(F) \cap V(F_X) \cap V(F_Y)$

Όμως αφού F ανάγωγο. άρα $(F, F_X) = 1$ και αφού δεν έχουν κοινούς παράγοντες έπεται από την πρόταση 1.18 ότι $V(F) \cap V(F_X)$ πεπερασμένο.
Το γεγονός αυτό ισχύει μόνο στις 2 διαστάσεις. Για παράδειγμα θεωρούμε την υπερεπιφάνεια $F = X^2 - Y^3 \in k[X, Y, Z]$ Τότε το ιδεώδες $I = (F)$ είναι πρώτο και άρα $V(F)$ ανάγωγο. Όμως το $P = (0, 0, z)$ είναι πολλαπλό για κάθε $z \in k$. □

Τέλος θα δούμε μία ενδιαφέρουσα εφαρμογή που συνδέει την πολλαπλότητα σημείων με τους ιακωβιανούς πίνακες πολυωνυμικών απεικονίσεων.

Πρόταση 3.2. *Έστω $T : A^2 \to A^2$ μια πολυωνυμική απεικόνιση, $T(Q) = P$.*
(α) Τότε $m_Q(F^T) \geq m_P(F)$
(β) Έστω $T = (T_1, T_2)$. Ορίζουμε $J_QT = (T_{iX_j}(Q))$ ως τον Ιακωβιανό πίνακα της T στο Q. Ισχύει ότι $m_Q(F^T) = m_P(F)$ εάν J_QT αντιστρέψιμος.
(γ) Το αντίστροφο του (β) δεν ισχύει. (Θεωρείστε $T = (X^2, Y), F = Y - X^2, P = Q = (0, 0)$)

Απόδειξη. Μπορούμε χ.β.γ να θεωρήσουμε $P = (0, 0)$. Αν όχι, κάνουμε απλά την γνωστή μετατόπιση. Έστω $Q = (q_1, q_2)$, $F = F_m + ... + F_n, S = (X + q_1, Y + q_2)$
Τότε $m_P(F) = m, m_Q(F^T) = m_{(0,0)}((F^T)^S)$

Έστω $U = T \circ S$. Τότε $U(0, 0) = (0, 0)$. Εάν $U = (U_1, U_2)$ τότε $U_1(0, 0) = 0 \Rightarrow$το U_1 δεν έχει σταθερό όρο. Όμοια και για το U_2.
Συνεπώς $F^U = F_m(U_1, U_2) + ... + F_n(U_1, U_2) = H = H_s + H_{s+1} + ...$ όπου επειδή τα U_1, U_2 δεν έχουν σταθερούς όρους συμπεραίνουμε ότι είτε $H = 0$ ή $s \geq m$ (γιατί· Σκεφτείτε τα μονώνυμα πως θα λειτουργούν).

Όμως $H \neq 0$ γιατί $U^T \neq 0$ και S αφφινική αλλαγή συντεταγμένων. Συνεπώς $m_q(F^T) = m_{(0,0)}(H) = s \geq m = m_P(F)$

(β) $U = (T \circ S) = (T_1(X + q_1, Y + q_10, T_2(X + q_1, Y + q_1)))$

Έστω J_QT αντιστρέψιμος πίνακας. Θα δείξουμε ότι $J_{(0,0)}U = J_QT$ Πράγματι $U_{1X}(0, 0) = \frac{d}{dx}(T_1(X + q_1, Y + q_2))|_{(0,0)} = T_{1X}(Q)$. Όμοια και τα υπόλοιπα και άρα $J_{(0,0)}U = J_QT$. Έχουμε τον ιακωβιανό λοιπόν πίνακα

$$J_{(0,0)}U = \begin{bmatrix} U_{1X} & U_{1Y} \\ U_{2X} & U_{2Y} \end{bmatrix}_{(0,0)}$$

Όμως J_QT αντιστρέψιμος από υπόθεση, άρα $U_{1X}(0, 0) \neq 0$ ή $U_{1Y}(0, 0) \neq 0$ (Αν είναι και τα δύο 0 τότε η ορίζουσα είναι 0 άρα δεν είναι αντιστρέψιμος)

Έστω χ.β.γ ότι $U_{1X}(0, 0) \neq 0 \Rightarrow U_1 = aX + G_1$ όπου G_1 υφηλότερος όρος, $a \neq 0$.

Με ίδια λογική $U_{2X}(0, 0) \neq 0$ ή $U_{2Y}(0, 0) \neq 0$. Πάλι χ.β.γ έχτω $U_{2Y}(0, 0) \neq 0$.

Τότε $F^U = (F_m + ... + F_n)^U = F_m(U_1, U_2) + ...$
αλλά $F_m(U_1, U_2) = F_m(aX + H_1, bY + H_2) = L_m +$ υψηλότεροι όροι και άρα προκύπτει το επιθυμητό αποτέλεσμα.

(γ) Μία απλή επαλήθευση με το παράδειγμα που δίνει και προκύπτει αμέσως το ζητούμενο. □

3.2 Τοπικοί δακτύλιοι και πολλαπλότητες σημείων

Έστω F ανάγωγη επίπεδη καμπύλη και $P \in F$. Σε αυτή την παράγραφο θα συνδέσουμε την πολλαπλότητα του P, $m_P(F)$ με τον τοπικό δακτύλιο $\mathcal{O}_P(F)$. Θυμίζουμε ότι για να κατασκευάσουμε τον τοπικό δακτύλιο, πρέπει το $V(F)$ να είναι ποικιλότητα και γι αυτό το λόγο απαιτούμε η επίπεδη καμπύλη μας να είναι ανάγωγη. Για πρακτικούς λόγους, εάν $G \in k[X, Y]$ θα συμβολίζουμε με g την εικόνα του στο $\Gamma(F) = k[X, Y]/(F)$.

Θεώρημα 3.1. *Το P είναι απλό σημείο στην F αν-ν το $\mathcal{O}_P(F)$ είναι ΔΔΕ. Σε αυτή την περίπωση, εάν $L = aX + bY + c$ είναι οποιαδήποτε ευθεία που περνάει από το P που δεν είναι εφαπτόμενη της F στο P, τότε η εικόνα της l στο $\mathcal{O}_P(F)$ είναι ομοιομορφοποιητής για το $\mathcal{O}_P(F)$*

Η μεθοδολογία της απόδειξης του θεωρήματος είναι αρκετά σημαντική.

Απόδειξη. Έστω P απλό σημείο στην F και L ευθεία που περνάει από το P αλλά δεν είναι εφαπτόμενη στην F. Με κατάλληλη αφφινική αλλαγή συντεταγμένων μπορούμε να υποθέσουμε ότι $P = (0,0)$, Υ η εφαπτόμενη ευθεία και $L = X$ (πεοτ. 2.11- προτ 2.6). Αρκεί λοιπόν να δείξουμε ότι $M_P(F) = (x)$(πρόταση 2.12).

Από την πρόταση 2.19 έχουμε ότι στον $\mathcal{O}_P(A^n)$ για οποιαδήποτε επιλογή του P, ακόμα και αν δεν είναι απλό, ισχύει ότι $M = I\mathcal{O}$, για $I = (X,Y) \subset k[X,Y]$. Από την πρόταση 2.20 έχουμε ότι $\mathcal{O}_P(V) \cong \mathcal{O}_P(A^n)/I\mathcal{O}_P(A^n)$ και άρα $M_P(F) = (x,y)$.

Αφού η εφαπτόμενη ευθεία στην F είναι η Y και το $(0,0)$ είναι απλό σημείο, άρα η F είναι της μορφής $F = Y + F_2 + ... + F_n$. Φέρνοντας όλα τα Υ μαζί γράφουμε την F ως $F = YG - X^2H$, όπου $G = 1 + G_1 + ...$ και $H \in k[X]$. Τότε $yg = x^2h \in \Gamma(F)$ και άρα $y = x^2hg^{-1}$ αφού $g(p) \neq 0$. Συνεπώς $M_P(F) = (x,y) = (x)$ κύριο ιδεώδες όπως θέλαμε. □

Για να δείξουμε το αντίστροφο θα χρειαστούμε ένα θεώρημα που θα παρουσιάσουμε στη συνέχεια.

Εάν έχουμε λοιπόν απλό σημείο σε μια καμπύλη F, το $\mathcal{O}_P(F)$ είναι ΔΔΕ και άρα ορίζεται συνάρτηση τάξης στο $k(F)$ που θα την ονομάζουμε ord_P^F. Όταν το F είναι φιξαρισμένα μπορούμε για απλούστευση να γράφουμε ord_P. Αν $G \in k[X,Y]$ και g η εικόνα του στο $\Gamma(F)$ τότε θα γράφουμε $ord_P^F(G)$ αντί για $ord_P^F(g)$.

Κοιτώντας την προηγούμενη απόδειξη μπορούμε να υποθέσουμε ότι $P = (0,0), M_P(F) = (x)$ και Υ η εφαπτόμενη. Οποιαδήποτε ευθεία περνάει από το P πέραν της εφαπτόμενης είναι της μορφής $L = aX + bY, a \neq 0$. Όμως $ord_P(x) = 1$ ενώ είδαμε ότι $y = x^2hg^{-1}$ και άρα $ord_P(y) \geq 2$. Συνεπώς $ord_P(L) = ord_P(ax + by)$ και από την πρόταση 2.14 συμπεραίνουμε ότι $ord_P(L) = 1$. Αν L η εφαπτόμενη, όμως, τότε $ord_P(L) \geq 2$. Αυτό φυσικά ισχύει για οποιαδήποτε επιλογή σημείου και καμπύλης.

Με την συνάρτηση τάξης μπορούμε να κατηγοριοποιήσουμε τα απλά σημεία μιας καμπύλης.

Αν L η εφαπτόμενη της F στο P και $ord_P^F(L) \geq 3$ τότε το P λέγεται <u>σημείο καμπής</u> (<u>flex</u>) . Αν ισχύει ισότητα τότε λέγεται <u>κανονικό σημείο καμπήςρ</u> (<u>ordinary</u>) αλλιώς λέγεται σημείο υψηλότερης καμπής (<u>higher flex</u>)

Πρωτού συνεχίσουμε στο επόμενο σημαντικό θεώρημα χρειάζεται να παρουσιάσουμε δύο πολύ απλά λήμματα που προκύπτουν από στοιχειώδη συνδιαστική.

Πρόταση 3.3. *(α) Υπάρχουν $d+1$ μονώνυμα βαθμού d στο $k[X,Y]$ και $1+2+....+(d+1) = \dfrac{(d+1)(d+2)}{2}$ μονώνυμα βαθμού d στο $k[X,Y,Z]$*
(β) Έστω $V(d,n)$ ={ομογενές βαθμού d στο $k[X_1,...,X_n]$ }.Τότε $V(d,n)$ είναι διανυσματικό χώρος πάνω από το k και τα πολυώνυμα βαθμού d αποτελούν βάση. $\dim V(d,1) = 1, \dim V(d,2) = d+1, \dim V(d,3) = \dfrac{(d+1)(d+2)}{2}$
(γ) $V(d,n) = \binom{d+n-1}{n-1}$

Η απόδειξη προκύπτει από μία απλή καταμέτρηση και στο (γ) απλή επαγωγή.

Πρόταση 3.4. *Έστω $I = (X,Y) \subset k[X,Y]$. Τότε* $\dim_k(k[X,Y]/I^n) = 1 + 2 + ... + n = \frac{n(n+1)}{2}$

Απόδειξη. Το I^n θυμίζουμε ότι παράγεται από τα μονώνυμα βαθμού n και αποτελείται από τα πολυώνυμα που δεν έχουν κανέναν όρο βαθμού $< n$. Συνεπώς οι εικόνες των πολυωνύμων βαθμού $< n$ παράγουν τον χώρο $k[X,Y]/I^n$. Μάλιστα αποτελούν βάση του παίρνοντας έναν γραμμικό τους συνδιασμό αμέσως βλέπουμε ότι αποτελούν βάση του.
Από την παραπάνω πρόταση έχουμε ότι υπάρχουν $d+1$ βαθμού d στον $k[X,Y]$ και άρα $1 + ... + (n-1+1) = 1 + ... + n = \frac{n(n+1)}{2}$ μονώνυμα βαθμού $\leq n-1$. □

Η απόδειξη του επόμενου θεωρήματος παρουσιάζει μία τεχνική που θα την χρησιμοποιούμε κατά κόρον από εδώ και στο εξής. Μας επιτρέπει να υπολογίζουμε τις διαστάσεις ορισμένων διανυσματικών χώρων της μορφής $\mathcal{O}_P(V)/I$ όπου I ιδεώδες στο $\mathcal{O}_P(V)$.

Θεώρημα 3.2. *Έστω P σημείο σε μια ανάγωγη καμπύλη F. Τότε $m_P(F) = \dim_K(M_P(F)^n/M_P(F)^{n+1})$ για κάθε αρκετά μεγάλο n (δείτε απόδειξη για το τι σημαίνει αυτό). Συγκεκριμένα, η πολλαπλότητα της F στο P εξαρτάται μόνο από τον τοπικό δακτύλιο $\mathcal{O}_P(F)$*

Απόδειξη. Γράφουμε για απλούστευση $\mathcal{O}, M$ αντί για $\mathcal{O}_P(F), M_P(F)$.

Δημιουργούμε την ακριβή ακολουθία

$$0 \to M^n/M^{n+1} \to \mathcal{O}/M^{n+1} \to \mathcal{O}/M^n \to 0$$

(είναι ακριβής από την πρόταση 2.22). Αρκεί να δείξουμε ότι για κάθε $n \geq m_P(F)$, ισχύει ότι $\dim_k(\mathcal{O}/M^n) = nm_P(F) + s$ για κάποια σταθερά s. Τότε επειδή η ακολουθία είναι ακριβής θα έχουμε ότι $\dim_k(M^n/M^{n+1}) = \dim_k(\mathcal{O}/M^{n+1}) - \dim_k(\mathcal{O}/M^n) = m_P(F)$.

Μπορούμε να υποθέσουμε ότι $P = (0,0)$ και άρα $M^n = I^n\mathcal{O}$ όπου $I = (X,Y) \subset k[X,Y]$ (πρόταση 2.17). Αφού $V(I^n) = \{P\}$ για κάθε $n \geq 0$ άρα $V(I^n, F)$ πεπερασμένο και άρα από το θεώρημα 2.1 έχουμε ότι $k[X,Y]/(I^n,F) \cong \mathcal{O}_P(A^n)/(I^n,F)\mathcal{O}_P(A^n) \overset{\text{πρόταση}2.20}{\cong} \mathcal{O}_P(F)/I^n\mathcal{O}_P(F) \overset{\text{πρότ } 2.19}{=} \mathcal{O}/M^n$

Μένει λοιπόν να υπολογίσουμε την διάσταση $k[X,Y]/(I^n,F)$. Τώρα πρέπει να περιοριστούμε για $n \geq m$ Έστω $m = m_P(F)$. Τότε $FG \in I^n$ για κάθε $G \in I^{n-m}$. Υπάρχει ένας φυσικός ομομορφισμός $\phi : k[X,Y]/I^n \to k[X,Y](I^n,F)$ και μια $k-$ γραμμική απεικόνιση $\psi : k[X,Y] \to I^{n-m} \to k[X,Y]/I^n$ που ορίζεται ως $\psi(\bar{G}) = \overline{FG}$

Εύκολα ελέγχουμε ότι η ακολουθία

$$0 \to k[X,Y]/I^{n-m} \xrightarrow{\psi} k[X,Y]/I^n \xrightarrow{\phi} k[X,Y]/(I^n,F) \longrightarrow 0$$

είναι ακριβής. Συνεπώς έχουμε από την πρόταση 3.4 ότι $\dim_k(k[X,Y]/(I^n,F)) = nm - \dfrac{m(m-1)}{2}$ για κάθε $n \geq m$ όπως θέλαμε.

□

Παρατηρείστε ότι αν το $\mathcal{O}_P(F)$ είναι ΔΔΕ, τότε από την πρόταση 2.23 έχουμε ότι $\dim_k(M^n/M^{n+1}) = 1$ και άρα $m_P(F) = 1$ που μας δίνει την αντίστροφη κατεύθυνση στο προηγούμενο θεώρημα.

Να αναφέρουμε ότι η συνάρτηση χ(n)=$\dim_k(\mathcal{O}/M^n)$, η οποία είναι πολυώνυμο του n (για μεγάλα n) λέγεται Hilbert Samuel πολυώνυμο του τοπικού δακτυλίου $\mathcal{O}$. Παίζει σημαντικό ρόλο στην μοντέρνα μελέτη των τοπικών δακτυλίων. Θα το μελετήσουμε περισσότερο και παρακάτω σε ασκήσεις/προτάσεις.

Εφαρμογές Για να δούμε την χρησιμότητα της μεθοδολογίας της απόδειξης θα εξασκηθούμε πρώτα σε μερικές εφαρμογές.

Για αρχή ας δούμε τι γίνεται εάν το n δεν είναι αρκετά μεγάλο, δηλαδή εάν $n \leq m_P(F)$.

Εφαρμογή 3.1. *Με τον συμβολισμό του παραπάνω θεωρήματος και θεωρώντας $M = M_P(F)$ να δείξετε ότι $\dim_k(M^n)/M^{n+1} = n+1$ για $0 \leq n \leq m_P(F)$. Συγκεκριμένα το P είναι απλό σημείο αν-ν $\dim_k(M/M^2)$=1, αλλιώς $\dim_k(M/M^2) = 2$.*

Απόδειξη. Ακολουθώντας την απόδειξη του παραπάνω θεωρήματος, έχουμε ότι η ακολουθία

$$0 \longrightarrow M^n/M^{n+1} \longrightarrow \mathcal{O}/M^{n+1} \longrightarrow \mathcal{O}M^n \longrightarrow 0$$

είναι ακριβής και $\mathcal{O}/M^n \cong k[X,Y]/(I^n,F)$, όπου $I = (X,Y) \subset k[X,Y]$.

Όμως εάν $F = F_m + ... + F_s$ και $m \geq n+1$ τότε $F \in I^{n+1}$ (άρα $\in I^n$ επίσης)και άρα $(I^n, F) = (I^n) \Rightarrow \mathcal{O}/M^n \cong k[X,Y]/I^n$.
Αλλά $\dim_k k[X,Y]/I^n = \dfrac{n(n+1)}{2}$ και συνεπώς $\dim_k(M^n/M^{n+1}) = \dim_k k[X,Y]/I^{n+1} - \dim_k k[X,Y]/I^n = n+1$.

Αν $\dim_k(M/M^2) = 1 \neq 2$ σημαίνει ότι $n = 1 \not< m \Rightarrow n = m = 1 \Rightarrow P$ απλό σημείο.

Αντίστροφα, εάν P απλό σημείο τότε $m_P(F) = 1$ και άρα το $n = 1$ είναι ¨αρκετά μεγάλο' ώστε να ισχύει το παραπάνω θεώρημα και άρα $m_P(F) = 1 = \dim_k(M^n/M^{n+1})$.

□

Αξίζει να μελετήσουμε λίγο παραπάνω και το πολυώνυμο Hilbert-Samuel .

Εφαρμογή 3.2. *(α) Έστω $\mathcal{O} = \mathcal{O}_P(A^n)$ για κάποιο $P \in A^2, M = M_P(A^2)$. Να υπολογιστεί το $\chi(n) = \dim_k(\mathcal{O}/M^n)$.*
(β) Έστω $\mathcal{O} = \mathcal{O}_P(A^r(k))$. Να δείξετε ότι το $\chi(n)$ είναι πολυώνυμο βαθμού r με πρωταρχικό συντελεστή $\frac{1}{r!}$.

Απόδειξη. (α) Χωρίς βλάβη γενικότητας υποθέτουμε ότι $P = (0,0)$. Έχουμε δει ότι ισχύει $M^n = I^n\mathcal{O}$ όπου $I = (X,Y)$ και αφού $V(I^n) = \{P\}$ άρα είναι πεπερασμένο και άρα $k[X,Y]/I^n \cong \mathcal{O}/I^n = \mathcal{O}M^n$ και $\dim_k k[X,Y]/I^n = \dfrac{n(n+1)}{2}$.

(β) Όμοια έχουμε ότι $\dim_k k[X_1,...,X_r]/I^n =$\{πλήθος μονωνύμων βαθμού $< n$\}$\overset{\text{πρόταση 3.4}}{=}$

$$\sum_{i=1}^{n-1} \binom{i+r-1}{r-1} = \binom{n+r-1}{r} = \frac{(n+r-1)}{r!(n-1)!} = \frac{n(n+1)\cdot ....\cdot(n+r-1))}{r!}$$

και άρα ο πρωταρχικός συντελεστής είναι όντως $\frac{1}{r!}$.

□

Εφαρμογή 3.3. *Έστω ότι $f \in k[X_1,...,X_r]$ ορίζει υπερεπιφάνεια στον A^r. Γράφουμε το $F = F_m + F^{m+1} + ...$ και ορίζουμε $m = M_P(F), P = (0,...,0)$. Έστω F ανάγωγο και $\mathcal{O} = \mathcal{O}_P(V(F))$, M το μέγιστο ιδεώδες. Να δείξετε ότι $\chi(n) = \dim_k(\mathcal{O}/M^n)$ είναι πολυώνυμο βαθμού $r-1$ για αρκετά μεγάλο n και ότι ο πρωταρχικός συντελεστής του χ είναι το $\frac{m_P(F)}{(r-1)!}$.*
Μπορείτε να βρείτε έναν άλλον ορισμό για την πολλαπλότητα ενός τοπικού δακτυλίου που να βγάζει νόημα σε όλες τις μέχρι τώρα γνωστές περιπτώσεις;

Απόδειξη. Κάνουμε ακριβώς την ίδια απόδειξη όπως αυτή του θεωρήματος. Θα έχουμε τότε ότι $\mathcal{O}/M^n \cong k[X_1,...,X_r]/(I^n, F)$ όπου $I = (X_1,...,X_r)$ και για $n \geq m$ η ακολουθία

$$0 \longrightarrow k[X_1,...,X_r]/I^{n-m} \longrightarrow k[X_1,...,X_r]/I^n \longrightarrow k[X_1,...,X_r]/(I^n, F) \longrightarrow 0$$

είναι ακριβής και άρα $\chi(n) = \dim_k k[X_1,...,X_r]/I^n - \dim_k k[X_1,...,X_r]/I^{n-m}$.
Όμως

$$\dim_k k[X_1,...,X_r]/I^n = \binom{n+r-1}{r} = \frac{n(n+1)...(n+r-1)}{r!} = \frac{1}{r!}(n^r + \frac{r(r-1)}{2}n^{r-1} + ...)$$

και

$$\dim_k k[X_1,...,X_r]/I^{n-m} = \binom{n-m+r-1}{r} = \frac{(n-m)....(n-m+r-1)}{r!} = \frac{1}{r!}(n^r + \frac{r(-2m+r-1)}{2}r^{n-1} + ...)$$

Αφαιρώντας κατά μέλη προκύπτει

$$\frac{m}{(r-1)!}n^{r-1} + ...$$

όπως θέλαμε.
Γενικά για έναν τοπικό δακτύλιο $\mathcal{O}$ με μέγιστο ιδεώδες M μπορούμε να θεωρήσουμε ως πολλαπλότητα του $\mathcal{O}$ τον αρχικό συντελεστή του $\chi(n)$ πολλαπλασιασμένο με $(r-1)!$ (για αρκετά μεγάλο n). Αμέσως παρατηρούμε ότι ο ορσιμός αυτός ταυτίζεται με τις γνωστές μας περιπτώσεις. □

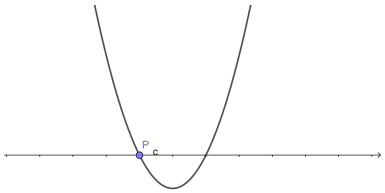
3.3 Αριθμοί τομής

Φτάσαμε στη πιο ενδιαφέρουσα παράγραφο του κεφαλαίου. Σε αυτή την παράγραφο θα προσπαθήσουμε να παρουσιάσουμε με αυστηρό τρόπο την πολλαπλότητα ενός σημείου τομής δύο καμπυλών F, G όπως είδαμε στην εισαγωγή. Στο 5ο κεφάλαιο θα γενικεύσουμε αυτή τη μέθοδο στον προβολικό χώρο και θα καταλήξουμε στο θεώρημα του Bezout .

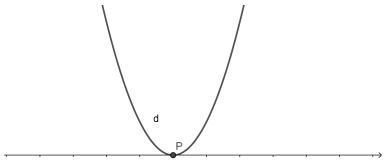
Η πολλαπλότητα του σημείου τομής δύο καμπυλών λέγεται **αριθμός τομής** (**intersection number**) και συμβολίζεται $i_P(F, G)$. Υπάρχει βέβαια ολόκληρος κλάδος πάνω σε αυτό το αντικείμενο που λέγεται intersection theory . Ο ορισμός είναι άμεσος και δίνεται από τον τύπο $i_P(F, G) = \dim_k(\mathcal{O}_P(A^2)/(F, G)$ αλλά αυτό δεν μας δίνει καμία διαίσθηση του πώς προέκυψε.

Αντιθέτως θα προσπαθήσουμε να αποκτήσουμε μία γεωμετρική διαίσθηση του αριθμού τομής μέσα από 9 κανόνες που θα θέλαμε να ισχύουν. Οι 7 από τους 9 κανόνες μάλιστα είναι αρκετοί ώστε να ορίζουν μονοσήμαντα μία μόνο συνάρτηση που τους ικανοποιεί η οποία δεν είναι άλλη από τον επίσημο ορισμό που δώσαμε.

Θα λέμε ότι οι καμπύλες F, G τέμνονται γνήσια στο P εάν δεν έχουν κανένα κοινό παράγοντα που να περνάει από το P. Η μελέτη μας θα είναι σε τέτοιες περιπτώσεις όπου η τομή είναι γνήσια.



Σχήμα 3.7: $i_P(F, G) = 1$



Σχήμα 3.8: $i_P(F, G) = 2$

Η διαίσθησή μας και μόνο θα μας έλεγε ότι οι δύο καμπύλες στο σχήμα 3.7 τέμνονται στο P ¨μία φορά' ενώ στο σχήμα 3.8, ¨δύο φορές' ενώ σε οποιοδήποτε άλλο σημείο που ανήκει μόνο στην μία καμπύλη και όχι στην άλλη, τέμνονται 0 φορές. Αν μετακινήσουμε τις καμπύλες ταυτόχρονα στον χώρο (αφφινική αλλαγή συντεταγμένων)επίσης δεν θα περιμέναμε να αλλάξει κάτι στο σημείο τομής τους. Στο σχήμα 3.8 παρατηρούμε επιπλέον ότι η καμπύλη F που εδώ είναι η ευθεία, ταυτίζεται με την εφαπτομένη της καμπύλης G (παραβολής) στο $P = (0, 0)$. Εξαιτίας αυτού, όπως θα δούμε το $i_P(F, G)$ είναι μεγαλύτερο απ ότι στο σχήμα 3.7 παρότι πρόκειται για τις ίδιες καμπύλες. Με μόνο αυτές τις διαισθητικές παρατηρήσεις μπορούμε να εξάγουμε τους 6 πρώτους κανόνες.

(1) Το $i_P(F, G)$ είναι μη αρνητικός ακέραιος για κάθε F, G και P τ.ω οι F, G να τέμνονται γνήσια στο P. Ορίζουμε $i_P(F, G) = \infty$ εάν δεν τέμνονται γνήσια στο P.

(2) $i_P(F, G) = 0$ αν-ν $P \notin F \cap G$. Το $i_P(F, G)$ εξαρτάται μόνο από τους παράγοντες των F, G που περνάνε από το P.

(3) Αν T αφφινική αλλαγή συντεταγμένων στο A^2 και $T(Q) = P$, τότε $i_Q(F^T, G^T) = i_P(F, G)$

(4) $i_P(F, G) = i_P(G, F)$

Δύο καμπύλες F και G λέμε ότι τέμνονται transversally στο P αν P απλό σημείο και στις δύο καμπύλες και εάν η εφαπτόμενη της F στο P είναι διαφορετική της εφαπτομένης της G στο P. Θέλουμε ο αριθμός της τομής να είναι ακριβώς 1 όταν οι F και G τέμνονται transversally . Γενικότερα, θέλουμε

(5) $i_P(F, G) \geq m_P(F)m_P(G)$ με την ισότητα να ισχύει αν-ν οι F και G <u>δεν έχουν</u> κοινές εφαπτομένες στο P

Ο αριθμός τομής πρέπει να προστίθεται όταν παίρνουμε ενώσεις καμπυλών

(6) Αν $F = \prod F_i^{r_i}, G = \prod G_j^{s_j}$, τότε $i_P(F, G) = \sum_{i,j} r_i s_j i_P(F_i, G_j)$

Ο 7ος κανόνας είναι ο λιγότερο διαισθητικός αλλά και ο περισσότερο χρήσιμος. Εάν η F είναι ανάγωγη, θέλουμε το $i_P(F, G)$ να εξαρτάται μόνο από την εικόνα του G στο $\Gamma(F)$ δηλαδή να λειτουργεί $modF$ κατά κάποιον τρόπο. Γενικά δηλαδή, θέλουμε

(7) $i_P(F, G) = i_P(F, G + AF)$ για κάθε $A \in k[X, Y]$

Αυτοί οι κανόνες είναι πλέον αρκετοί.

Θεώρημα 3.3. *Υπάρχει μοναδική συνάρτση $i_P(F, G)$ που ορίζεται για όλες τις επίπεδες καμπύλες F, G και όλα τα σημεία $P \in A^2$ και που να ικανοποιεί τις ιδιότητες (1)-(7). Δίνεται από τον τύπο $i_P(F, G) = \dim_k(\mathcal{O}_P(A^n)/(F, G))$*

Πριν μιλήσουμε για την απόδειξη να αναφέρουμε και δύο επιπλέον κανόνες που προκύπτουν ως συμπεράσματα.

(8) Αν P απλό σημείο τότε $i_P(F, G) = ord_P^F(G)$

(9) Αν F, G δεν έχουν κοινούς παράγοντες, τότε $\sum_P i_P(F, G) = \dim_k(k[X, Y]/(F, G))$

Ο τελευταίο κανόνας προκύπτει απλά από το λήμμα 2.3 .Η γενίκευση του τελευταίου κανόνα στον προβολικό χώρο αποτελεί το θεώρημα του Bezout

Για το (8) υποθέτουμε ότι F ανάγωγο. Αν g η εικόνα της G στο $\mathcal{O}_P(F)$, τότε από την πρόταση 2.23 έχουμε $ord_P^F(G) = \dim_k(\mathcal{O}_P(F)/(g))$. Όμως από την πρόταση 2.20 έχουμε ότι $\mathcal{O}_P(F)/(g) \cong \mathcal{O}_P(A^n)/(F, G) = i_P(F, G)$

Τα βήματα για την απόδειξη του θεωρήματος είναι πρώτον να αποδείξουμε την μοναδικότητα και δεύτερον να αποδείξουμε ότι η συνάρτηση $\dim_k(\mathcal{O}_P(A^n)/(F, G))$ επαληθεύει και τους 7 κανόνες. Η μόνη πραγματική δυσκολία παρουσιάζεται στον 5ο κανόνα, το οποίο χρειάζεται αρκετό κόπο για να αποδειχτεί. Την απόδειξη, παρόλο ενδιαφέρουσα θα την παραλείψουμε καθώς είναι αρκετά τεχνική.

Εφαρμογές

Πρόταση 3.5. *Έστω P διπλό σημείο σε μια καμπύλη F και έστω ότι η F έχει μία μόνο εφαπτομένη L στο P.*
(α) Να δείξετε ότι $i_P(F, L) \geq 3$. Η F λέγεται ότι έχει αιχμηρό σημείο αν $i_P(F, L) = 3$.
(β) Αν $P = (0, 0)$ και $L = Y$ να δείξετε ότι το P είναι αιχμηρό σημείο αν-ν $F_{XXX} \neq 0$. Να δώσετε παραδείγματα.
(γ) Να δείξετε ότι αν το P αιχμηρό στην F, τότε η F έχει μόνο έναν παράγοντα που να περνάει από το P.

Απόδειξη. Υποθέτουμε όπως πάντα χ.β.γ ότι $P = (0, 0)$. Αφού P διπλό σημείο άρα $F = F_2 + F_3 + ... + F_n$.

Η F έχει μόνο μία εφαπτομένη L και άρα $F_2 = L^2 = (aX + bY)^2$

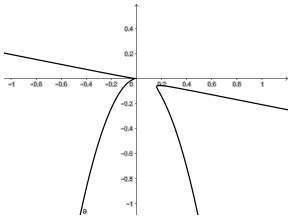
(α) Αφού L κοινή εφαπτομένη των F, L άρα $i_P(F, L) > m_P(F)m_P(L) = 2$ και άρα $i_P(F, L) \geq 3$

(β) Έστω $F = Y^2 + F_3 + ... + F_n$

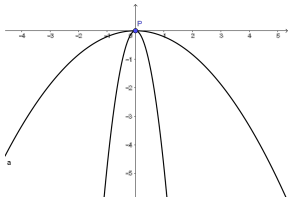
$i_P(Y, F) = i_P(Y, F - Y^2) = i_P(Y, F_3 + ... + F_n) \geq 3$

$i_P(Y, F) = 3 \Leftrightarrow Y \nmid F_3 \Leftrightarrow F_3 = X^3 + ... \Leftrightarrow F_{3XXX} \neq 0 \Leftrightarrow F_{XXX} \neq 0$

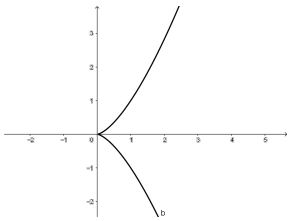
Παραδείγματα: $F_1 = Y^2 + X^3 + 5X^2Y$. Έχει αιχμηρό σημείο στο $P = (0,0)$ ενώ η $F_2 = Y^2 + 5X^2Y + X^4$ δεν έχει αιχμηρά σημεία. Το πιο απλό και διάσημο παράδειγμα αιχμηρού σημείου είναι η $F_3 = Y^2 - X^3$



Σχήμα 3.9: $F_1 = Y^2 + X^3 + 5X^2Y$



Σχήμα 3.10: $F_2 = Y^2 + 5X^2y + X^4$



Σχήμα 3.11: $F_3 = Y^2 - X^3$

(γ) Έστω P αιχμηρό σημείο και $F = GH$ τ.ω $G(P) = H(P) = 0$. Πάλι υποθέτουμε ότι $L = Y$ και $P = (0,0)$ Τότε $i_P(Y,G) > 0$ και $i_P(Y,H) > 0$ αφού $P \in Y \cap G \cap H$. Όμως $i_P(Y,F) = 3 = i_P(Y,G) + i_P(Y,H)$ και άρα αναγκαστικά $i_P(Y,F) = 1$ και $i_P(Y,H) = 2$.

Όμως $i_P(Y,G) = 1 \Rightarrow G = X + aY + G_2 + \ldots$, $a \in k$ και
$i_P(Y,H) = 2 \Rightarrow H = Y + H_2 + \ldots$ ή $H = X^2 + \ldots$. Όμως $F = Y^2 + X^3 + \ldots$ οπότε σε οποιαδήποτε περίπτωση είναι άτοπο. □

Πρόταση 3.6. *Μία ευθεία L είναι εφαπτόμενη σε μία καμπύλη F στο P αν-ν $i_P(F,L) > m_P(F)$.*

Απόδειξη. Από ιδιότητα (5) έχουμε ότι $i_P(F,L) > m_P(F)m_P(L) = m_P(F) \Leftrightarrow F, L$ δεν έχουν κοινή εφαπτομένη $\Leftrightarrow L$ όχι εφαπτόμενη της F. □

Κεφάλαιο 4

Προβολικές Ποικιλότητες

Πριν μπούμε στο κεφάλαιο της προβολικής γεωμετρίας χρειάζεται πολύ σύντομα να αναπτύξουμε κάποια βασικά εργαλεία με τα ομογενή πολυώνυμα.

4.1 Ομογενή Πολυώνυμα

Ως τώρα είχαμε αποφύγει να μιλήσουμε πολύ για τα ομογενή πολυώνυμα αλλά μερικές ιδιότητές τους είναι πλέον απαραίτητες για να συνεχίσουμε

Έστω R ακεραία περιοχη. Αν $F \in R[X_1, ..., X_{n+1}]$ είναι ομογενές, τότε ορίζουμε $F_* = F(X_1, ..., X_n, 1)$. Ανάποδα για οποιοδήποτε πολυώνυμο $f \in R[X_1, ..., X_n]$ βαθμού d, όπου $f = f_0 + f_1 + ... + f_d$, f_i ομογενές βαθμού i ορίζουμε $f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + ... + f_d$. Το f^* είναι ομογενές βαθμού d. Αυτές οι διαδικασίες μπορούν να χαρακτηρισθούν ως ομογενοποίηση και απομογενοποίηση (homogenize-dehomogenize) ως προς X_{n+1}

Πρόταση 4.1. *1.* $(FG)_* = F_* G_*, \quad (fg)^* = f^* g^*$

2. $(F+G)_* = F_* + G_* \quad X_{n+1}^t (f+g)^* = X_{n+1}^r f^* + X_{n+1}^s g^*$, *όπου* $r = \deg(g), s = \deg(f), t = r + s - \deg(f+g)$

3. Αν r η υψηλότερη δύναμη του X_{n+1} που διαιρεί το F, τότε $X_{n+1}^r (F_*)^* = F, \quad (f^*)_* = f$

Λήμμα 4.1. *Ως προς δυνάμεις του X_{n+1}, η παραγοντοποίση ενός ομογενούς $F \in R[X_1, ..., X_{n+1}]$ είναι το ίδιο με την παραγοντοποίηση του $F_* \in R[X_1, ..., X_n]$. Συγκεκριμένα, εάν $F \in k[X, Y]$ είναι ομογενές και k αλγεβρικά κλειστό, τότε το F παραγοντοποιείται σε γινόμενο γραμμικών παραγόντων.*

Το τελευταίο λήμμα για τις δύο διαστάσεις το έχουμε ήδη χρησιμοποιήσει ως δεδομένο μέχρι τώρα κι έχουμε δώσει και αντιπαράδειγμα για να δείξουμε ότι το ίδιο δεν ισχύει σε μεγαλύτερες διαστάσεις. (πριν την πρόταση 3.1)

Οι αποδείξεις προκύπτουν αμέσως από τους ορισμούς οπότε παραλείπονται

Θα αναφέρουμε και ένα χρήσιμο κριτήριο για να ελέγχουμε εάν ένα πολυώνυμο είναι ανάγωγο, πρωτού προχωρήσουμε παρακάτω

Πρόταση 4.2. *Έστω $F, G \in k[X_1, ..., X_n]$ ομογενή βαθμού $r, r+1$ αντίστοιχα χωρίς κοινούς παράγοντες (k σώμα). Τότε $F + G$ ανάγωγο*

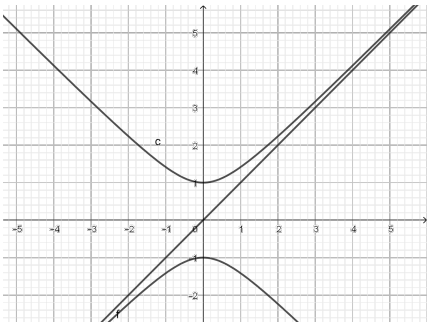
Απόδειξη. Η απόδειξη είναι άμεση. Έστω $F = F_r, G = G_{r+1}$ και $F_r + G_{r+1} = TH = (T_0 + ... + T_a)(H_0 + ... + H_b)$. Με στοιχειώδεις πράξεις καταλήγουμε σε άτοπο. □

Η πρόταση είναι εξαιρετικά χρήσιμη καθώς μας επιτρέπει να ελέγχουμε αμέσως κατά πόσον πολυώνυμα της μορφής $F_n + F_{n+1}$ είναι ανάγωγα(π.χ το $F = X^2 + Y^3 + Y^2X + 5X^2Y$ μπορούμε αμέσως να πούμε ότι είναι ανάγωγο).

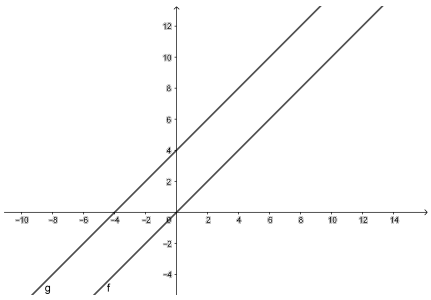
4.2 Προβολικός Χώρος

Όπως έχουμε ήδη εξηγήσει στην εισαγωγή, ο λόγος που εισάγουμε την προβολική γεωμετρία είναι για να λύσουμε το πρόβλημα της παραλληλίας ή των ασύμπτωτων καμπυλών.

Για παράδειγμα στα δύο επόμενα σχήματα



Σχήμα 4.1: ασύμπτωτες



Σχήμα 4.2: παράλληλες

θέλουμε να βρούμε έναν ¨καλό' τρόπο ώστε να μπορούμε να πούμε ότι οι 2 καμπύλες να τέμνονται (στο άπειρο).

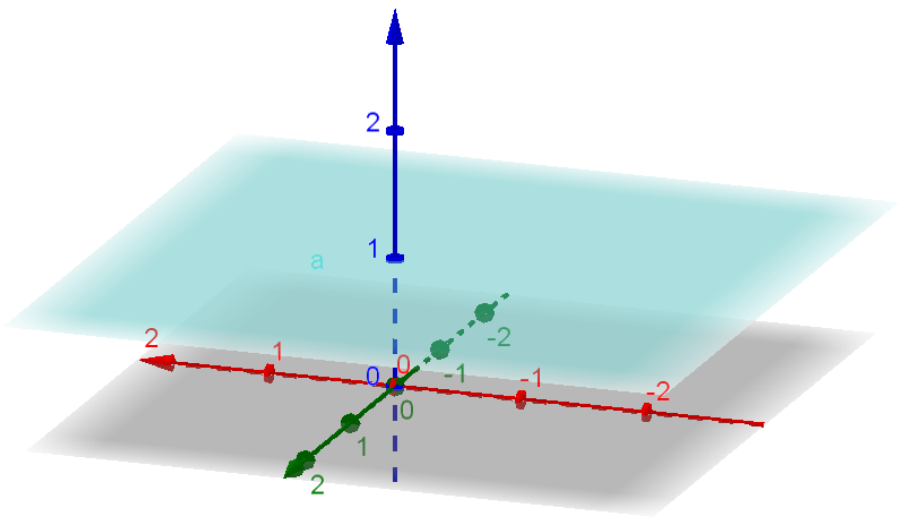
Υπάρχουν αρκετοί τρόποι να ορίσει κανείς τον προβολικό χώρο. Ο πιο διαισθητικός ίσως είναι ο εξής. Ας ξεκινήσουμε με τον A^2 και θα κατασκευάσουμε τον P^2. Τον A^2 τον σκεφτόμαστε ως το γνωστό μας αφφινικό επίπεδο. Για να φτιάξουμε τον προβολικό χώρο, προσθέτουμε μία επιπλέον διάσταση, τον άξονα των z και ανεβάζουμε το επίπεδό μας στο ύψος $z = 1$ όπως στο σχήμα

Το επίπεδο αυτό παραμένει αφφινικό. Στο επίπεδο αυτό τα πάντα παραμένουν ίδια με μόνη εξαίρεση ότι τώρα θα προσθέσουμε την έννοια του απείρου. Το πιο απλό παράδειγμα για να το καταλάβουμε είναι η ευθεία. Συνδέουμε κάθε σημείο της ευθείας με το $(0, 0, 0)$ και δημιουργείται έτσι ένα υπερεπίπεδο του οποίου η τομή με το $z = 0$ δημιουργεί μία επιπλέον ευθεία. Διαλέγουμε τυχαία ένα σημείο της ευθεία αυτής ως αντιπρόσωπο και λέμε ότι το σημείο αυτό είναι το σημείο της αρχικής ευθεία στο άπειρο. Το επίπεδο $z = 0$ το σκεφτόμαστε δηλαδή ως διανυσματικό χώρο και ταυτίζουμε τα διανύσματά του που ανήκουν στην ίδια ευθεία.

Στον προβολικό χώρο δηλαδή θεωρούμε τις ευθείες που περνάνε από το $(0, 0, 0)$ ως σημεία.
Τώρα που αποκτήσαμε μία διαίσθηση ας το ορίσουμε και πιο αυστηρά.

Έστω k σώμα. Ονομάζουμε προβολικό $n-$ χώρο και το συμβολίζουμε με $P^n(k)$, ή P^n για συντομία, το σύνολο όλων των ευθειών που περνάνε από το $(0, ..., 0)$ το A_k^{n+1}. Ένα οποιοδήποτε σημείο $x = (x_1, ..., x_{n+1}) \neq (0, ..., 0)$ ορίζει μια μοναδική ευθεία, την $\{(\lambda x_1, ..., \lambda x_{n+1}) | \lambda \in k\}$. Δύο τέτοια σημεία $(x), (y)$ ορίζουν την ίδια ευθεία αν-ν υπάρχει $\lambda \in k, \lambda \neq 0$ τ.ω $y_i = \lambda x_i$ για κάθε $i = 1, ..., n + 1$. Σε αυτή την περίπτωση τα δύο αυτά σημεία τα θεωρούμε ισοδύναμα και τα ταυτίζουμε. Έτσι ο P^n ορίζεται ως το σύνολο των κλάσεων ισοδυναμίας των σημείων του $A^{n+1} - \{(0, ..., 0)\}$.

Τα στοιχεία του P^n λέγονται σημεία. Εάν ένα σημείο $P \in P^n$ ορίζεται από κάποια $(x_1, ..., x_{n+1}) \in A^{n+1}$, λέμε τότε ότι το $(x_1, ..., x_{n+1})$ είναι σύνολο ομογενών συντεταγμένων για το P. Συχνά γράφουμε $P = (x_1, ..., x_{n+1})$ για να δείξουμε ότι το $(x_1, ..., x_{n+1})$ είναι ομογενείς συντεταγμένες για το P. Παρατηρείστε ότι η κάθε μία συντεταγμένη από μόνη της δεν είναι καλά ορισμένη αφού για παράδειγμα $(x_1, ..., xn + 1) = (2x_1, ..., 2x_{n+1})$. Όμως, μπορούμε να πούμε με ασφάλεια εάν η συντεταγμένη x_i είναι ίση ή διάφορη του 0



Σχήμα 4.3

καθώς και να μιλήσουμε για την αναλογία x_j/x_i (αφού αυτές οι ιδιότητες παραμένουν αναλοίωτες με την κλάση ισοδυναμίας).

Ορίζουμε $U_i = \{(x_1, ..., x_{n+1}) \in P^n | x_i \neq 0\}$. Κάθε $P \in U_i$ έχει μοναδικό σύνολο ομογενών συντεταγμένων της μορφής $P = (x_1, ..., x_{i-1}, 1, x_{x+1}, ..., x_{n+1})$. Οι συντεταγμένες $\{(x_1, ..., x_{i-1}, x_{i+1}, ..., x_{n+1})\}$ λέγονται μη-ομογενείς συντεταγμένες του P ως προς το U_i(ή συνηθέστερα ως προς το X_i, ή το i). Εάν ορίσουμε $\phi_i : A^n \to U_i, \quad \phi_i(a_1, ..., a_n) = (a_1, ..., a_{i-1}, a_{i+1}, ..., a_{n+1})$ τότε βλέπουμε εύκολα ότι ϕ_i είναι ισομορφισμός και άρα $A^n \cong U_i$. Παρατηρούμε επίσης ότι $P^n = \bigcup_{i=1}^{n+1}$ και άρα το P^n καλύβεται από $n+1$ σύνολα που το καθένα είναι ισόμορφο με τον αφφινικό $n-$ χώρο.

Συνήθως για ευκολία επικεντρονώμαστε κυρίως στο U_{n+1} Θεωρούμε επίσης $H_\infty = P^n - U_{n+1} = \{(x_1, ..., x_{n+1}) | x_{n+}$ $0\}$. Το H_∞ λέγεται υπερεπίπεδο στο άπειρο και μπορεί να ταυτιστεί με το P^{n-1} μέσω της αντιστοίχισης $(a_1, ..., a_n, 0) \leftrightarrow (a_1, ..., a_n)$.
Συνεπώς $P^n = U_{n+1} \cup H_\infty$ και άρα το P^n μπορεί να θεωρηθεί ως ένωση ενός αφφινικού $n-$ χώρου και ενός συνόλου που δίνει όλες τις κατευθύνσεις στον αφφινικό $n-$ χώρο. Θα γίνει αρκετά πιο ξεκάθαρο από ασκήσεις που θα δούμε στη συνέχεια. Η επόμενη πρόταση είναι ο οικοδομικός λίθος για την επόμενη παράγραφο.

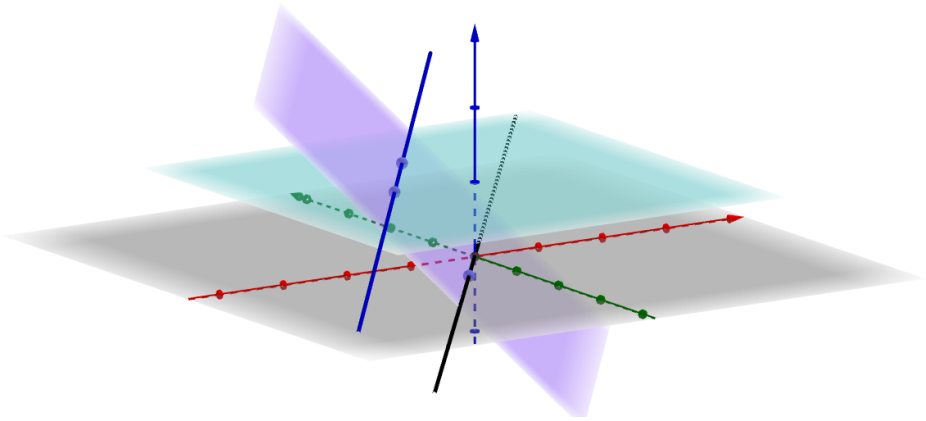
Πρόταση 4.3. *Έστω $F \in k[X_1, ..., X_{n+1}]$, ($k$ άπειρο) και $F = \sum F_i$ όπου F_i ομογενή. Έστω $P \in P^n(k)$ και $F(x_1, ..., x_{n+1}) = 0$ για κάθε επιλογή ομογενών συντεταγμένων του P. Τότε για κάθε ομογενές ισχύει $F_i(x_1, ..., x_{n+1}) = 0$ για κάθε επιλογή ομογενών συντεταγμένων του P.*

Απόδειξη. Έστω $P \in P^n$ και $F(P) = 0 \Rightarrow F(\lambda p_1, ..., \lambda p_{n+1}) = 0 \quad \forall \lambda \in k - \{0\} \Rightarrow \sum_i F_i(\lambda p_1, ..., \lambda p_{n+1}) = 0$.

Όμως $F_i = \sum a_i X_1^{b_{i1}} .... X_n^{b_{in}}, b_{i1} + ... + bin = i$ και άρα $F_i(\lambda x_1, ..., \lambda X_n) = \lambda^i F_i(x_1, ..., x_{n+1})$

Άρα $F(p_1, ..., p_{n+1}) = \sum \lambda^i F_i(p_1, ..., p_{n+1}) = 0 \forall \lambda \in k, \lambda \neq 0$.

Αν $F_i(p_1, ..., p_{n+1}) \neq 0$ για κάποιο i τότε το πολυώνυμο $G(\lambda) = \sum \lambda^i F_i(p_1, ..., p_{n+1})$ δεν είναι μηδενικό και άρα έχει πεπερασμένο αριθμό ριζών (το πολύ $n+1$). Όμως το k είναι άπειρο και $G(\lambda) = 0 \forall \lambda \in k$ και άρα άτοπο. Συνεπώς $F_i(p_1, ..., p_{n+1}) = 0$ για κάθε i και για κάθε επιλογή συντεταγμένων του P. □



Σχήμα 4.4

4.3 Προβολικά Αλγεβρικά Σύνολα

Τόσο σε αυτή όσο και στην επόμενη παράγραφο θα προσπαθήσουμε να επεκτείνουμε όσα έχουμε μάθει μέχρι τώρα, στον προβολικό χώρο. Θα ξεκινήσουμε φυσικά με την πιο βασική έννοια τα αλγεβρικά σύνολα και τα βασικά θεωρήματα γύρω από αυτά. Καθώς οι αποδείξεις είναι παρόμοιες με αυτές στον αφφινικό χώρος θα τις παραλείπουμε, επιμένοντας περισσότερο στα αποτελέσματα.

Ένα σημείο $P \in P^n$ λέμε ότι μηδενίζει το πολυώνυμο $F \in k[X_1, ..., X_{n+1}]$ εάν $F(x_1, ..., x_{n+1}) = 0$ για κάθε επιλογή ομογενών συντεταγμένων του P. Γράφουμε τότε $F(P) = 0$. Αν γράψουμε το F ως άθροισμα ομογενών πολυωνύμων, τότε κάθε ομογενές σύμφωνα με την πρόταση 4.3 θα μηδενίζει στο P.

Για ένα οποιοδήποτε σύνολο πολυωνύμων στο $k[X_1, ..., X_{n+1}]$, ορίζουμε $V(S) = \{P \in P^n | P \text{μηδενίζει κάθε} F \in S\}$. Στον αφφινικό χώρο ίσχυε ότι $V(S) = V(I(S))$. Εδώ ισχύει, χάρη στην προηγούμενη πρόταση κάτι ακόμα πιο ισχυρό. Εάν $I = I(S) = (F^{(1)}, ..., F^{(r)})$ και $F^{(i)} = \sum F_j^{(i)}$, όπου $F_j^{(i)}$ ομογενές βαθμού j, τότε $V(I) = V(\{F_j^{(i)}\}) = V(S)$, δηλαδή παράγεται από ομογενή. Ένα τέτοιο σύνολο λέγεται προβολικό αλγεβρικό σύνολο.

Για οποιοδήποτε σύνολο $X \subset P^n$ ορίζουμε όμοια $I(X) = \{F \in k[X_1, ..., X_{n+1}] | F(P) = 0 \forall P \in X\}$ και ονομάζεται ιδεώδες του X.

Ένα ιδεώδες I ονομάζεται ομογενές εάν για κάθε $F \in I$ με $F = \sum F_i$ το άθροισμά του σε ομογενή, ισχύει ότι $F_i \in I$ για κάθε i. Προφανώς το $I(X)$ είναι ομογενές ιδεώδες για κάθε σύνολο X.

Πρόταση 4.4. *Ένα ιδεώδες $I \subset k[X_1, ..., X_{n+1}]$ είναι ομογενές εάν-ν παράγεται από (πεπερασμένο) σύνολο από ομογενή πολυώνυμα.*

Η απόδειξη είναι άμεση από τους ορισμούς και παραλείπεται.

Ένα αλγεβρικό σύνολο $V \subset P^n$ λέγεται ανάγωγο εάν δεν μπορεί να γραφεί ως ένωση δύο μικρότερων αλγεβρικών συνόλων. Στους αφφινικούς χώρους είχαμε ότι V ανάγωγο αν-ν $I(V)$ πρώτο. Το ίδιο ισχύει κι εδώ αλλά για να το ισχυριστούμε αυτό χρειαζόμαστε πρώτα μία πρόταση

Πρόταση 4.5. *Έστω I ομογενές ιδεώδες στο $k[X_1, ..., X_{n+1}]$. Το I είναι πρώτο αν-ν ισχύει το εξής: για κάθε ομογενές $F, G \in k[X_1, ..., X_{n+1}]$, αν $FG \in I$ τότε $F \in I$ ή $G \in I$*

Απόδειξη. Η μία κατεύθυνση είναι προφανής. Για την άλλη, υποθέτουμε ότι ισχύει η συνθήκη και έστω $F, G \in k[X_1, ..., X_{n+1}]$ τ.ω $FG \in I$. Αρκεί να δείξουμε ότι $F \in I$ ή $G \in I$. Έστω, λοιπόν, ότι δεν ισχύει. Γράφουμε $F = F_m + ... + F_n, G = G_s + ... + G_l$. Τότε αφού $F \notin I$ άρα υπάρχει F_i τ.ω $F_i \notin I$ και

όμοια G_j τ.ω $G_j \notin I$. Διαλέγουμε τα μικρότερα δυνατά τέτοια F_i, G_j. Τότε αναπτύσσοντας το γινόμενο $H = FG$ σε άθροισμα από ομογενών πολυωνύμων και παρατηρώντας το H_{i+j} ομογενές βαθμού $i+j$ έχουμε ότι $H_{i+j} = F_iG_j + T$ όπου $T \in I$ (διαλέξαμε τα μικρότερα δυνατά F_i, G_j ώστε να μπορούμε να ισχυριστούμε ότι $T \in I$). Όμως από την συνθήκη έχουμε ότι $F_iG_j \notin I$ και άρα $H_{i+j} \notin I$. Όμως, αφού I ομογενές και έχουμε υποθέσει ότι $FG \in I$ άρα $H_{i+j} \in I$ που είναι άτοπο.

□

Με αυτή την πρόταση πια, εύκολα δείχνουμε ότι στον προβολικό χώρο ισχύει, όπως στον αφφινικό, ότι V ανάγωγο αν-ν $I(V)$ πρώτο. Έναν ανάγωγο αλγεβρικό σύνολο λέγεται προβολική ποικιλότητα . Κάθε προβολικό αλγεβρικό σύνολο μπορεί να γραφεί ως ένωση από προβολικές ποικιλότητες, τους ανάγωγους παράγοντές του.

Το διάγραμμα

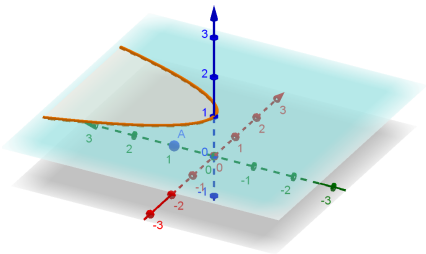
Γεωμετρία		**Άλγεβρα**
$P^n(k)$		$k[X_1, ..., X_{n+1}]$
{Προβολικά κλειστά/αλγεβρικά υποσύνολα}	$\longleftrightarrow$	{ριζικά ιδεώδη}.
$\bigcup$		$\bigcup$
{ Προβολικές ποικιλότητες }	$\longleftrightarrow$	{πρώτα ιδεώδη}
$\bigcup$		$\bigcup$
P^n_k={ σημεία στον P^n_k} $\ni (a_1, ..., a_n, a_{n+1})$	$\longleftrightarrow$	{μέγιστα ιδεώδη } $\ni m = (X_1 - a_1, ..., X_n - a_n)$

εξακολουθεί να ισχύει με μόνη εξαίρεση ότι τα ιδεώδη εδώ είναι ομογενή.

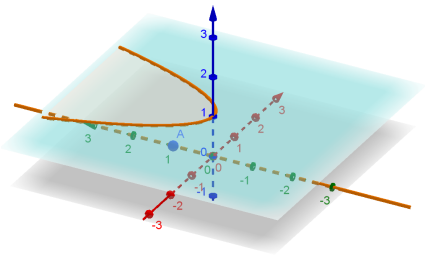
Την κατεύθυνση πρώτα ιδεώδη με ποικιλότητες την αναφέραμε παραπάνω. Η αντιστοίχιση των μέγιστων ιδεωδών με τα σημεία είναι επίσης σχετικά απλή να δειχτεί. Αυτό που θέλει παραπάνω αιτιολόγηση είναι η αντιστοίχιση των ριζικών ιδεωδών με τα αλγεβρικά σύνολα που θα την δείξουμε λίγο παρακάτων.

Έως τώρα έχουμε χρησιμοποιήσει τους ίδιους συμβολισμούς $V(X), I(V)$ όπως στον αφφινικό χώρο. Παρ΄ όλ΄ αυτά οι έννοιες αυτές εν γένει είναι διαφορετικές ανάμεσα στον προβολικό και αφφινικό χώρο και πρέπει να γίνεται ξεκάθαρη διάκριση όποτε χρειάζεται. Θα γράφουμε λοιπόν V_p, I_p για τον προβολικό και V_a, I_a για τον αφφινικό.

Εάν το V είναι αλγεβρικό σύνολο στο P^n ορίζουμε $C(V) = \{(x_1, ..., x_{n+1}) \in A^{n+1} | (x_1, ..., x_{n+1}) \in V \quad \text{ή } (x_1, ..., x_{n+1}) = (0, ..., 0)\}$ ως τον κώνο πάνω από το V. Το $C(V)$ δεν είναι τίποτα άλλο παρά η αφφινική εποπτεία που έχουμε εμείς στα σχήματα του P^n. Και το όνομα βέβαια δεν είναι τυχαίο. Για παράδειγμα ένα σχήμα στο P^2 με την προβολική εποπτεία είναι το παρακάτω

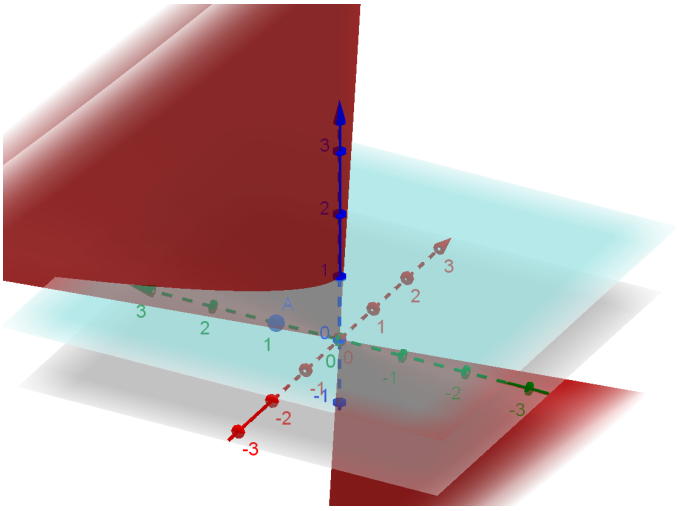


Σχήμα 4.5: $yz = x^2$ προβολική εποπτεία



Σχήμα 4.6: Προβολική εποπτεία. Η πορτοκαλί ευθεία υποδηλώνει την ευθεία που τείνει να μοιάσει η παραβολή στο άπειρο

Προβολικά παρατηρούμε ότι το σχήμα μας είναι απλά η παραβολή $y = x^2$ υπεριψωμένη στο επίπεδο $z = 1$ μαζί με ένα σημείο της στο άπειρο. Αφφινικά όμως αυτό που θα βλέπαμε θα ήταν ένας κώνος (4.7)



Σχήμα 4.7: αφφινική εποπτεία=$C(V)$

Αν $V \neq \emptyset$, τότε $I_a(C(V)) = I_p(V)$ και αν I ομογενές ιδεώδες στο $k[X_1, ..., X_{n+1}]$ τ.ω $V_p(I) \neq \emptyset$, τότε $C(V_p(I)) = V_a(I)$. Αυτή η παρατήρηση ανάγει πολλές ερωτήσεις για το P^n σε ερωτήσεις για το A^{n+1}. Μπορούμε λοιπόν έτσι να γενικεύσουμε το Nullstellensatz απαντώντας έτσι και στο ερώτημα με την αντιστοίχιση των αλγεβρικών συνόλων με τα ριζικά ιδεώδη.

Θεώρημα 4.1 (Projective Nullstellensatz). *Έστω I ομογενές ιδεώδες στο $k[X_1, ..., X_{n+1}]$. Τότε*

1. *$V_p(I) = \emptyset$ αν-ν υπάρχει ακέραιος N τ.ω το I να περιέχει όλα τα ομογενή πολυώνυμα βαθμού $\geq N$*
2. *Αν $V_p(I) \neq \emptyset$, τότε $I_p(V_p(I)) = \sqrt{I}$*

Απόδειξη. 1. Από τις παρατηρήσεις που κάναμε προηγουμένως προκύπτει ότι $V_p(I) = \emptyset \Leftrightarrow V_a(I) \subset \{(0, ..., 0)\} \Leftrightarrow \sqrt{I} = I_a(V_a(I)) \supset (X_1, ..., X_{n+1})$ (από αφφινικό Nullstellensatz) $\overset{\text{προτ. } 2.16}{\Leftrightarrow} (X_1, ..., X_{n+1})^N \supset I$ για κάποιο $N \in \mathbb{N}$.

2. $I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = \sqrt{I}$

□

Να παρατηρήσουμε, βέβαια, ότι εάν το I είναι ομογενές, τότε και το $\sqrt{I}$ είναι ομογενές. Πράγματι εάν $F \in \sqrt{I}$ και $F + F_m + ... + F_n$, τότε $\exists N \in \mathbb{N} : F^N \in I \Rightarrow (F_m + ... + F_n)^N \in I$. Όμως $(F_m + ...F_n)^N = F_m^N +$ υψηλότεροι όροι. Όμως I ομογενές άρα $F_m^N \in I$. Συνεχίζουμε έπειτα και με τα υπόλοιπα ομογενή επαγωγικά και προκύπτει το ζητούμενο.

Έστω V προβολική ποικιλότητα στο P^n. Το $I(V)$ είναι πρώτο ιδεώδες, οπότε ο δακτύλιος $\Gamma_h(V) = k[X_1, ..., X_{n+1}]/I(V)$ είναι ακεραία περιοχή και λέγεται ομογενές δακύλιος συντεταγμένων .

Πιο γενικά, εάν I ομογενές ιδεώδες στο $k[X_1, ..., X_{n+1}]$, τότε θεωρούμε $\Gamma = k[X_1, ..., X_{n+1}]/I$. Ένα στοιχείο $f \in \Gamma$ θα καλείται ομογενές βαθμού d εάν υπάρχει ομογενές F βαθμού d στο $k[X_1, ..., X_{n+1}]$ που η εικόνα του να κάνει f.

Πρόταση 4.6. *Κάθε στοιχείο $f \in \Gamma$ μπορεί να γραφεί μοναδικά ως $f = f_0 + ... + f_m$, f_i ομογενές βαθμού i.*

Αυτή την ανάλυση φυσικά δεν μπορούμε να την κάνουμε (διατηρώντας τη μοναδικότητα) για μη ομογενή ιδεώδη.

Απόδειξη. Αν f είναι η εικόνα του F στο $k[X_1, ..., X_{n+1}]$, τότε γράφουμε το F ως $F = \sum F_i$ και τότε $f = \sum f_i$. όπου f_i οι εικόνες των F_i. Το σημαντικό είναι να δείξουμε την μοναδικότητα. Έστω $f = \sum g_i$, g_i εικόνα του G_i. Τότε $F - \sum G_i = \sum(F_i - G_i) \in I$ και αφού I ομογενές άρα $F_i - G_i \in I$ για κάθε i και άρα $f_i = g_i$. □

Με $k_h(V)$ συμβολίζουμε το σώμα κλασμάτων του $\Gamma_h(V)$ και λέγεται ομογενές σώμα συναρτήσεων . Θυμίζουμε ότι στον αφφινικό χώρο, κάθε στοιχείο του $\Gamma(V)$ εξέφραζε μία απεικόνιση από το V στο k. Παρόλαυτά, το ίδιο δεν μπορεί να θεωρηθεί κι εδώ, καθώς το $f \in \Gamma_h(V)$ μπορεί να στέλνει διαφορετικές συντεταγμένες του $P = (p_1, ..., p_{n+1})$ σε διαφορετικά σημεία, δηλαδή μπορεί για παράδειγμα να ισχύει ότι $f(p_1, ..., p_{n+1}) \neq f(2p_1, ..., 2p_{n+1})$ κ.ο.κ. Όμοια τα περισσότερα στοιχεία του $k_h(V)$ δεν μπορούν να θεωρηθούν ως συναρτήσεις. Παρ΄ όλ΄ αυτά αν f, g είναι ομογενή ίδιου βαθμού στο $\Gamma_h(V)$ τότε το f/g ορίζει όντως συνάρτηση, τουλάχιστον στα σημεία όπου δεν μηδενίζει το g, καθώς $\frac{f(\lambda x)}{g(\lambda x)} = \frac{\lambda^d f(x)}{\lambda^d g(x)} = \frac{f(x)}{g(x)}$ και άρα το $\frac{f}{g}$ είναι ανεξάρτητο της επιλογής των ομογενών συντεταγμένων.

Το σώμα συναρτήσεων του V, που γράφεται $k(V)$ ορίζεται ως το σύνολο $\{z \in k_h(V) | z = \frac{f}{g}$για κάποια ομογενή f, g | Εύκολα ελέγχουμε ότι το $k(V)$ είναι υπόσωμα του $k_h(V)$ και μάλιστα ισχύει $k \subset k(V) \subset k_h(V)$, αλλά $\Gamma_h(V) \nsubseteq k(V)$. Στοιχεία του $k(V)$ ονομάζονται ρητές συναρτήσεις στο V.

Έστω $P \in V, z \in k(V)$. Λέμε ότι το z ορίζεται στο P εάν μπορεί να γραφτεί ως $z = f/g, f, g$ ομογενή ίδιου βαθμού και $g(P) \neq 0$. Ορίζουμε $\mathcal{O}_P(V) = \{z \in k(V) : z$ορίζεται στο P $\}$. Το $\mathcal{O}_P(V)$ είναι υποδακτύλιος του $k(V)$, είναι τοπικός με μέγιστο ιδεώδες το $M_P(V) = \{z | z = f/g, g(P) \neq 0, f(P) = 0\}$. Η τιμή $z(P)$ είναι προφανώς καλά ορισμένη για $z \in \mathcal{O}_P(V)$

Εάν $T : A^{n+1} \to A^{n+1}$ είναι γραμμική αλλαγή συντεταγμένων, τότε το T μεταφέρει ευθείες που περνάνει από το κέντρο των αξόνων σε ευθείες που επίσης περνάνε από το κέντρο (πρόταση 2.6). Συνεπώς το T ορίζει μία απεικόνιση από το P^n στο P^n που λέγεται προβολική αλλαγή συντεταγμένων . Εάν το V είναι αλγεβρικό, τότε το $T^{-1}(V) = V^T$ είναι επίσης αλγεβρικό. Εάν $V = V(F_1, ..., F_r)$ τότε $V^T = V(F_1^T, ..., F_r^T)$ όπου T_i ομογενές βαθμού 1.

Όλα τα υπόλοιπα γνωστά θεωρήματα μεταφράζονται στον προβολικό χώρο με παρόμοιο τρόπο. Συνολικά η βασική αλγεβρική διαφορά του προβολικού από τον αφφινικό χώρο είναι ότι πλέον δουλεύουμε με ομογενή πολυώνυμα και ιδεώδη και γραμμικές αλλαγές συντεταγμένων. Καταλαβαίνουμε λοιπόν πόσο σημαντικό είναι να μπορούμε να ομογενοποιούμε ένα πολυώνυμο καθώς και να εκτελούμε και την ανάποδη διαδικασία, να μεταβαίνουμε δηλαδή από τον αφφινικό χώρο A^n στον προβολικό P^n και ανάποδο. Η μέθοδος αυτή θα αναπτυχθεί στην επόμενη παράγραφο.

Εφαρμογές Ξεκινάμε με μία ωραία άσκηση/πρόταση για τους κώνους. Θα χρειαστούμε πρώτα ένα γνωστό λήμμα από την αντιμεταθετική άλγεβρα:

Λήμμα 4.2. *Αν p πρώτο ιδεώδες και I_1, I_2 ιδεώδες τ.ω $I_1 \cap I_2 \subset p$, τότε $I_1 \subset p$ ή $I_2 \subset p$.*

Πρόταση 4.7. *Κάθε ανάγωγος παράγοντας ενός κώνου είναι κώνος.*

Απόδειξη. Έστω $V = \bigcup_{i=1}^n V_i$, όπου V_i ανάγωγο αλγεβρικό υποσύνολο στο P^n.

$C(V) = C(\cup_i V_i) = \{(x_1, ..., x_{n+1}) \in A^{n+1} | (x_1, ..., x_{n+1}) \in \cup V_i$ή$(x_1, ..., x_{n+1}) = (0, ..., 0)\} = \cup C(V_i)$

Αρκεί να δείξουμε ότι $C(V_i)$ είναι ανάγωγα. Ισοδύναμα, αρκεί να δείξουμε ότι εάν V ανάγωγο στο P^n τότε $C(V)$ ανάγωγο στο A^{n+1}.

Έστω $C(V) = X_1 \cup X_2$ όπου X_i ανάγωγα(όμοια εάν ήταν περισσότερα σύνολα στην ένωση, χρησιμοποιούμε απλά δύο για απλούστευση).

Τότε $I_a(C(V_i)) = I_a(X_1 \cup X_2) \Rightarrow I_p(V) = I_a(X_1) \cap I_a(X_2)$.

Όμως $I_p(V)$ είναι πρώτο ιδεώδες και $I_a(X_1) \cap I_a(X_2) \subset I_p(V)$ και άρα από το λήμμα έχουμε ότι $I_a(X_1) \subset I_P(V)$ ή $I_a(X_2) \subset I_p(V)$. Καταλήγουμε ότι $I_p(V) = I_a(X_1)$. άρα $V_a(I_p(V)) = V_a(I_a(X_1)) \Rightarrow C(V) = X_1$ όπως θέλαμε. □

Η επόμενη πρόταση είναι γενίκευση της πρότασης 2.6. Αρχικά ο αντίστοιχος ορισμός της ευθείας

Ορισμός 4.1. *Έστω $P = (a_1, ..., a_{n+1})$, $Q = (b, ..., b_{n+1})$ διακεκριμένα σημεία του P^2. Η ευθεία L που περνάει από το P και Q ορίζεται ως $L = \{(\lambda a_1 + \mu b_1, ..., \lambda a_{n+1} \mu b_{n+1}) | \lambda, \mu \in k, \lambda \neq 0 ή \mu \neq 0\}$*

Πρόταση 4.8.

1. *Αν L ευθεία που περνάει από τα P, Q και T γραμμική αλλαγή συντεταγμένων τότε $T(L)$ η προβολική ευθεία που περνάει από τα $T(P), T(Q)$*

2. *Η ευθεία είναι γραμμική υποποικιλότητα διάστασης 1 αλλά και ότι ένα γραμμική υποποικιλότητα διάστασης 1 αποτελέι ευθεία που περνά από οποιαδήποτε δύο της σημεία.*

3. *Στο P^2 η ευθεία ταυτίζεται με το υπερεπίπεδο.*

4. *Έστω $P, P' \in P^2, L_1, L_2$ ευθείες που περνάνε από το P και L'_1, L'_2 ευθείες που περνάνε από το P'. Τότε υπάρχει γραμμική αλλαγή συντεταγμένων T τ.ω $T(P) = P'$ και $T(L_i) = L'_i, i = 1, 2$*

Η απόδειξη είναι αρκετά παρόμοια με αυτή της πρότασης 2.6 οπότε παραλείπεται. Παρ΄ όλ΄ αυτά, με βάση αυτή την πρόταση μπορούμε να εξάγουμε αρκετά, σημαντικά συμπεράσματα.

Πρόταση 4.9. *Έστω P_1, P_2, P_3 μη συνευθειακά σημεία και Q_1, Q_2, Q_3 επίσης μη συνευθειακά. Τότε υπάρχει μοναδική προβολική αλλαγή συντεταγμένων $T : P^2 \to P^2$ τ.ω $T(P_i) = Q_i, i = 1, 2, 3$*

Απόδειξη. Η απόδειξη είναι άμεση με γραμμική άλγεβρα. Έστω $P_i = (a_{i1}, a_{i2}, a_{i3})$ και $q_i = (q_{i1}, q_{i2}, q_{i3})$, $T = (T_1, T_2, T_3)$ όπου $T_i = b_{i1}X_1 + b_{i2}X_2 + b_{i3}X_3$.

Αν συμβολίσουμε με A τον πίνακα των p_i, T τον πίνακα των T_i και Q τον πίνακα των Q_i, παίρνουμε το σύστημα $AT = Q$. όμως επειδή p_i όχι συνευθειακά, άρα A είναι αντιστρέψιμος και άρα $T_i = QA^{-1}$. Αφού επιπλέον q_i μη συνευθειακά, άρα $detQ \neq 0 \Rightarrow \det T = \det Q \det A \neq 0$, άρα T καλά ορισμένη προβολική αλλαγή συντεταγμένων.

□

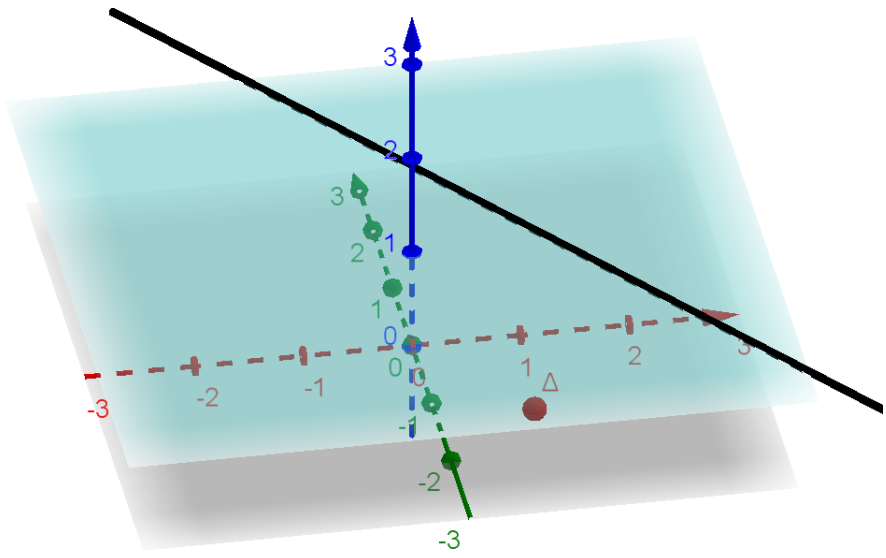
Πρόταση 4.10. *Δύο διακεκριμένες ευθείες στο P^2 τέμνονται σε ένα μόνο σημείο.*

Απόδειξη. Από την πρόταση 4.8 έχουμε ότι οι ευθείες ταυτίζονται με τα υπερεπίπεδα στο P^2 και άρα $L_1 = V(F), L_2 = V(G)$,όπου $F = a_1X + a_2Y + a_3Z$, $G = b_1X + b_2Y + b_3Z$, $\quad (a_1, a_2, a_3) \neq \lambda(b_1, b_2, b_3) \neq 0$.

Από γραμμική άλγεβρα έχουμε ότι το σύστημα $\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$

έχει άπειρες λύσεις της μορφής $(c_1, c_2, c_3)\mu \forall \mu \in k$ (θεώρημα βαθμού μηδενικότητας) και αυτές είναι και όλες οι λύσεις. Άρα $L_1 \cup L_2 = (c_1, c_2, c_3) \in P^2$. □

Αυτή η πρόταση είναι και ο βασικός λόγος που εισαγάγαμε την προβολική γεωμετρία. Για να έχουμε και μία γεωμετρική εποπτεία, η ευθεία στον P^2 είναι αυτής της μορφής.



Σχήμα 4.8

Αποτελείται δηλαδή από μία αφφινική ευθεία στο επίπεδο $z = 1$ και ένα σημείο στο διανυσματικό επίπεδο $z = 0$. Δύο λοιπόν προβολικές ευθείες, είτε θα τέμνονται στο αφφινικό επίπεδο $z = 1$ είτε θα είναι παράλληλες και θα τέμνονται στο διανυσματικό επίπεδο $z = 0$.

Πρόταση 4.11. *Έστω L_1, L_2, L_3 (αντ M_1, M_2, M_3) ευθείες στο P^2 που δεν περνάνε όλες από ένα σημείο. Τότε υπάρχει μοναδική αλλαγή προβολικών συντεταγμένων $T : P^2 \to P^2$ τ.ω $T(L_i) = M_i$.*

Απόδειξη. Από την πρόταση 4.10 έχουμε ότι οποιεσδήποτε δύο μη διακεκριμένες ευθείες τέμνονται σε ένα σημείο. Έστω $P_i = L_j \cap L_k$, $Q_i = M_j \cap M_k$ όπου i, j, k διακεκριμένα.

Τότε από προτ. 4.9 έχουμε ότι υπάρχει μονάδική προβολική αλλαγή συντ/νων τ.ω $T(P_i) = Q_i \Leftrightarrow T(L_j \cap L_k) = G_j \cap Q_k$. Από την προτ. 4.8 μία ευθεία ορίζεται μονοσήμαντα από δύο σημεία της. Η L_i ευθεία περνάει από τα P_j, P_k και η $T(L_i)$ ευθεία από τα Q_j, Q_k όπως και η M_i. Συνεπώς $T(L_i) = M_i$ για κάθε i. □

Πρόταση 4.12. *Έστω $H = V(\sum a_i X_i)$ υπερεπίπεδο στο P^n. Το $(a_1, ..., a_{n+1})$ καθορίζεται από το H (ως προς πολλαπλασιασμό με μία σταθερά).*

1. *Η αντιστοίχιση του $(a_1, ..., a_{n+1}) \in P^n$ στο H φτιάχνει μία φυσική 1-1 αντιστοιχία μεταξύ {υπερεπίπεδα στο P^n} και το P^n*

2. *Έστω $P \in P^n$ και P^* το αντίστοιχο υπερεπίπεδο. Αν H υπερεπίπεδο, το H^* δηλώνει το αντίστοιχο σημείο. Τότε $P^{**} = P, H^{**} = H$. Επιπλέον $P \in H \Leftrightarrow H^* \in P^*$.*
   Αυτή είναι η γνωστή δυϊκότητα του προβολικού χώρου.

Απόδειξη. Έστω $A =$ {υπερεπίπεδα στο P^n} και

$$\phi : P^n \to A, \quad p = (a_1, ..., a_n) \mapsto H = V(\sum a_i X_i)$$

Αμέσως δείχνεται ότι φ καλά ορισμένη 1-1 κι επί όπως ζητείται.

(2) Έστω $P = (a_1, ..., a_{n+1}) \Rightarrow H = V(\sum a_i X_i) = P^* \Rightarrow P^{**} = (a_1, ..., a_{n+1})$. Όμοια $H^{**} = H$.
Έστω $P \in H, P = (a_1, ..., a_{n+1}), H = V(\sum b_i X_i)$ Έχουμε ότι $P \in H \Rightarrow \sum b_i a_i = 0$
$P^* = V(\sum a_i X_i), H^* = (b_1, ..., b_{n+1})$
Αφού όμως $\sum a_i b_i = 0$ άρα $H^* \in P^*$. Όμοια για το αντίστροφο. □

4.4 Αφφινικές και Προβολικές ποικιλότητες

Μπορούμε να θεωρήσουμε το A^n ως υποσύνολο του P^n μέσω της απεικόνισης $\phi_{n+1} : A^n \to U_{n+1} \subset P^n$. Σε αυτή την παράγραφο θα μελέτησουμε τη σχέση των αλγεβρικών συνόλων του A^n με αυτά του P^n.

Έστω V ένα αλγεβρικό σύνολο στο A^n, $I = I(V) \subset k[X_1, ..., X_n]$. Έστω I^* το ιδεώδες του $k[X_1, ..., X_{n+1}]$ που παράγεται από τα $\{F^* | F\ inI\}$. Το I^* είναι ομογενές ιδεώδες. Ορίζουμε $V^* = V(I^*) \subset P^n$

Ανάποδα εάν Vαλγεβρικό στο P^n και $I = I(V) \subset k[X_1, ..., X_{n+1}]$ θεωρούμε το I_* ως το ιδεώδες στο $k[X_1, ..., X_n]$ που παράγεται από τα $\{F_* | F \in I\}$. Όμοια ορίζουμε $V_* = V(I_*) \subset A^n$. Ισχύουν οι επόμενες βασικές προτάσεις.

Πρόταση 4.13. *1. Αν $V \subset A^n$, τότε $\phi_1 n + 1(V) = V^* \cap U_{n+1}$ και $(V^*)_* = V$*

2. Αν $V \subset W \subset A^n$, τότε $V^* \subset W^* \subset P^n$. Αν $V \subset W \subset P^n$, τότε $V_* \subset W_* \subset A^n$.

3. Αν V ανάγωγο στο A^n τότε το V^*ανάγωγο στο P^n

4. Αν $V = \cup_i V_i$ η ανάλυση του V σε ανάγωγους παράγοντες στο A^n, τότε $V^* = \cup_i V_i^*$ η ανάλυση του P^n σε ανάγωγους παράγοντες στο P^n.

5. Αν $V \subset A^n$, τότε το V^* είναι το μικρότερο αλγεβρικό σύνολο στο P^n που περιέχει το V.

6. Αν $V \subsetneqq A^n$, τότε κανένας παράγοντας του V^* δεν κείται ή δεν περιέχει το $H_\infty = P^n - U_{n+1}$.

7. Αν $V \subset P^n$, και κανένας παράγοντας του V δεν κείται ή δεν περιέχει το H_∞, τότε $V_* \subsetneqq A^n$ και $(V_*)^* = V$

Οι αποδείξεις στις παραπάνω προτάσεις είναι άμεσες από τους ορισμούς, χρησιμοποιώντας ως οδηγό την πρώτη παράγραφο του κεφαλαίου, και συνεπώς παραλείπονται.

Αξίζει να επιμείνουμε λίγο περισσότερο στην πρόταση 5. Εάν το δούμε από τοπολογική σκοπιά και θυμηθούμε ότι τα αλγεβρικά σύνολα αντιστοιχούν σε κλειστά σύνολα στην τοπολογία μας, τότε η πρόταση 5 επαναδιατυπώνεται ως: Αν $V \subset A^n$ το $V*$ είναι η κλειστότητα του V (θυμίζουμε ότι το V το βλέπουμε ως υποσύνολο του P^n μέσα από την απεικόνιση ϕ_{n+1}). Μάλιστα ισχύει το επόμενο λήμμα.

Λήμμα 4.3. *Αν $I = (F)$ ιδεώδες μιας αφφινικής υπερεπιφάνειας, τότε $I^* = (F^*)$. Αυτό δεν ισχύει στην γενική περίπτωση $I = (F_1, ..., F_r)$.*

Απόδειξη. $I^* = \{G^* S \quad | G \in I, S \in k[X_1, ..., X_{n+1}]\} = \{(FH)^* S \quad | H \in k[X_1, ..., X_n]\} = \{F^*(H^* S)\} \overset{\text{για } H=1}{=} \{F^* S\} = (F^*)$.

Παρόλαυτα αν θεωρήσουμε $I = (F_1, F_2) = (Y - X^2, Z - X^3) \subset k[X, Y, Z]$, τότε $F_1^* = YW - X^2, F_2^* = ZW^2 - X^3$. Παρατηρούμε ότι $F_2 - XF_1 = Z - XY \in I \Rightarrow (F_2 - XF_1)^* = (Z - XY)^* = ZW - XY \in I^*$ αλλά εύκολα βλέπουμε ότι $ZW - XY \notin (F_1^*, F_2^*) = (YW - X^2, ZW^2 - X^3)$. Συνεπώς $I^* \neq (F_1^*, F_2^*)$.

□

Πέραν των προβολικών ποικιλοτήτων που κείτονται στο H_∞, υπάρχει μία 1-1 αντιστοίχιση μεταξύ των αφφινικών ποικιλοτήτων και των προβολικών γεγονός που προκύπτει από το (7) της παραπάνω πρότασης. Η μόνη περίπτωση που δεν εξετάζει είναι όταν $V \supset H_\infty$, όπου θα τη μελετήσουμε στα δύο επόμενα λήμματα, για τα οποία όμως θα χρειαστούμε πρώτα μία πρόταση από την αντιμεταθετική άλγεβρα.

Πρόταση 4.14. *Έστω R Π.Μ.Α και $P = (t)$ κύριο, γνήσιο, πρώτο ιδεώδες. Τότε δεν υπάρχει πρώτο ιδεώδες Q τ.ω $0 \subsetneq Q \subsetneq P$*

Απόδειξη. Αφού R Π.Μ.Α και $P = (t)$ πρώτο, άρα t ανάγωγο. Έστω ότι υπάρχει Q πρώτο ιδεώδες τ.ω $0 \subsetneq Q \subsetneq P$. Αφού $0 \subsetneq Q$ άρα υπάρχει $q \in Q, q \neq 0$. Όμως $Q \subset P \Rightarrow q \in P \Rightarrow \exists a \in R : q = at$
Αν $t \in Q$ τότε $P \subset Q$ που είναι άτοπο άρα $t \notin Q$. Όμως Q πρώτο και $at \in Q \Rightarrow a \in Q \Rightarrow a \in P$. Αν a ανάγωγο τότε $a = ut$ με u αντιστρέψιμο, που είναι άτοπο γιατί $t \notin Q$. Συνεπώς α όχι ανάγωγο. Αφού R Π.Μ.Α, άρα $\exists! p_1, ..., p_r$ ανάγωγα τ.ω $a = up_1^{n_1}, ..., p_r^{n_r}, uunit$. Επειδή η ανάλυση αυτή είναι μοναδική και $a \in (t)$ και t ανάγωγο συμπεραίνουμε ότι ένα από τα p_i είναι ίσο με t. Χ.Β.Γ υποθέτουμε $p_1 = t$. Τότε $a = t^{n_1}, ..., p_r^{n_r}$ και άρα $q = at = t^{n_1+1}p_2^{n_2}...p_r^{n_r} \in Q$.

Αφού Q πρώτο άρα τουλάχιστον ένας από τους παράγοντες αυτούς ανήκουν στο Q. Προφανώς $u \notin Q$ αφού Q γνήσιο ιδεώδες. Αν $t^{n_1+1} \in Q \Rightarrow t \in Q$ (Αφού Q πρώτο και άρα ριζικό) που είναι άτοπο. Συνεπώς $\exists p_i$ ανάγωγο τ.ω $p_i \in Q$. Τότε $p_i \in (t) \Rightarrow p_i = (t)$ που είναι άτοπο και άρα δείχτηκε το ζητούμενο. □

Λήμμα 4.4. *Αν $V \subset W \subset P^n$ ποικιλότητες και V υπερεπιφάνεια, τότε $W = V$ ή $W = P^n$.*

Απόδειξη. Αν $V = V(F)$ υπερεπιφάνεια, αφού είναι ποικιλότητα συμπεραίνουμε ότι $I(V) = (F)$ πρώτο (και κύριο) ιδεώδες. Αν $V \subset W \subsetneq P^n$, τότε $0 \subsetneq I(W) \subsetneq I(V)$ όπου $I(W)$ πρώτο ιδεώδες αφού W ποικιλότητα. Από την παραπάνω πρόταση καταλήγουμε σε άτοπο. □

.

Λήμμα 4.5. *Έστω $V \subset P^n$ προβολική ποικιλότητα και $H_\infty \subset V$. Τότε $V = P^n$ ή $V = H_\infty$. Αν $V = P^n$, $V_* = A^n$, ενώ εάν $V = H_\infty$, τότε $V_* = \emptyset$.*

Απόδειξη. Παρατηρούμε ότι $H_\infty = V(X_{n+1})$ υπερεπίπεδο και ποικιλότητα, άρα από το προηγούμενο λήμμα $V = P^n$ ή $V = H_\infty$.

Έστω $V = P^n$, τότε $V = V(0) \Rightarrow V_* = V(0) = A^n$.

Αν $V = V(X_{n+1}) \Rightarrow V_* = V(1) = \emptyset$. □

Τελειώνουμε την ενότητα γενικεύοντας τις έννοιες των τοπικών δακτυλίων στους προβολικούς χώρους.

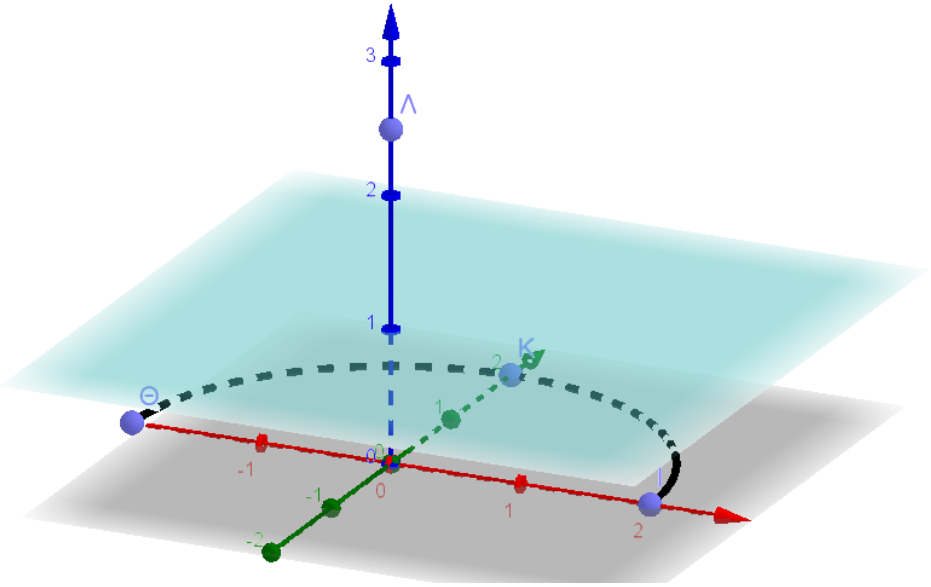
Έστω V αφφινική ποικιλότητα και $V^* \subset P^n$ η προβολική κλειστότητά του. Αν $f \in \Gamma_h(V^*)$ είναι ομογενές βαθμού d, ορίζουμε f_* ως εξής : Θεωρούμε ένα ομογενές $F \in k[X_1, ..., X_{n+1}]$ βαθμού d του οποίου η εικόνα του στο $I_p(V^*)$ είναι το f και ορίζουμε $f_* =$ εικόνα στο $I(V)$ του F_*(χρειάζεται κανείς να ελέγξει ότι αυτός ο ορισμός είναι ανεξάρτητος της επιλογής του F). Ορίζουμε τότε έναν φυσικό ισομορφισμό $a : k(V^*) \to k(V)$,όπου $a(f/g) = f_*/g_*$, με f, g ομογενή ίδιου βαθμού στο V^*. Αν $P \in V$, μπορούμε να θεωρήσουμε ότι $P \in V^*$ (μέσω της ϕ_{n+1} και τότε το a επάγει έναν ισομορφισμό μεταξύ του $\mathcal{O}_P(V^*)$ και του $\mathcal{O}_P(V)$. Συνήθως χρησιμοποιούμε το a για να ταυτίσουμε το $k(V)$ με το $k(V^*)$ και το $\mathcal{O}_P(V)$ με το $\mathcal{O}_P(V^*)$

Κάθε προβολική ποικιλότητα $V \subset P^n$ καλύβεται από $n + 1$ σύνολα $V \cap U_i$. Εάν σχηματίσουμε το V_* ως προς το U_i (αντί για το U_{n+1} που κάνουμε συνήθως), τότε τα σημεία του $V \cap U_i$ αντιστοιχούν σε σημεία του V_* και οι τοπικοί δακτύλιοι είναι ισόμορφοι. Συνεπώς ερωτήσει σχετικά με το V δίπλα από ένα σημείο μπορούν να μεταφραστούν σε ερωτήσεις σχετικά με ένα αφφινική ποικιλότητα V_* (τουλάχιστον εάν η ερώτηση μπορεί να απαντηθεί κοιτώντας το $\mathcal{O}_P(V)$).

Πρόταση 4.15. *Για οποιαδήποτε πεπερασμένη συλλογή σημείων στο P^2, υπάρχει ευθεία που δεν περνά μέσα από κανένα από αυτά.*

Απόδειξη. Η απόδειξη αυτής της πρότασης είναι καθαρά γεωμετρική και θα μας βοηθήσει να αποκτήσουμε μία καλύτερη εποπτεία του προβολικού χώρου. Θυμίζουμε ότι το P^2 μπορούμε να το σκεφτούμε ως δύο επίπεδα, το $z = 1$ που είναι αφφινικό και το $z = 0$ που είναι διανυσματικό με την σύμβαση ότι ταυτίζουμε τα διανύσματα που βρίσκονται στην ίδια ευθεία. Συγκεκριμένα στο P^2 το επίπεδο $z = 0$ μπορούμε να το σκεφτούμε ως

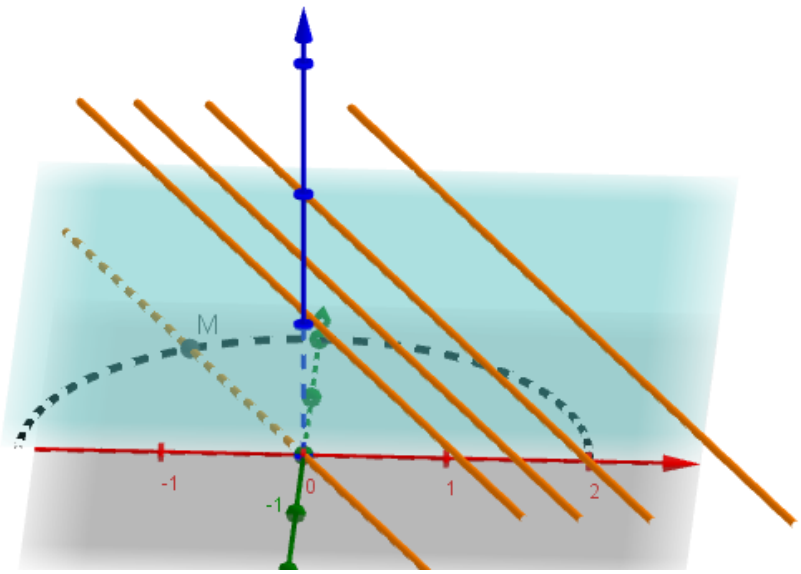
ημικύκλιο (δηλαδή θεώρουμε ως αντιπροσώπους της κλάσης ισοδυναμίας τα σημεία με μέτρο 1), (ή ως ευθεία αν σκεφτούμε τα σημεία να είναι της μορφής $P = (a, 1, 0)$) οπότε ο προβολικός χώρος P^2 μοιάζει με το σχήμα



Σχήμα 4.9

Κάθε σημείο του ημικυκλίου αντιστοιχεί σε μία οικογένεια παράλληλων ευθειών στο $z = 1$ και αντίστροφα. Το σημείο δηλαδή στο $z = 0$ εκφράζει την κλίση της ευθείας στο $z = 1$.

Με αυτές τις παρατηρήσεις γυρνάμε στην πρόταση. Έστω $A = \{P_1, ..., P_s\}$ ένα πεπερασμένο σύνολο από σημεία. Χωρίζουμε το A σε $A_0 = H_\infty \cap A$, δηλαδή τα σημεία στο επίπεδο $z = 0$, και A_1 τα υπόλοιπα. Δηλαδή $A_0 = \{P_i \in A : P_i = (a_i, b_i, 0)\}$ και $A_1 = \{P_j \in A : P_j = (a_j, b_j, 1)\}$. Προφανώς $A = A_0 \cup A_1$ και τα δύο σύνολα είναι ξένα μεταξύ τους. Αφού το A_0 πεπερασμένο, άρα μπορούμε να βρούμε τουλάχιστον ένα σημείο στο H_∞ που να μην ανήκει στο A_0 (αφού υποθέτουμε ότι το σώμα μας είναι αλγεβρικά κλειστό και άρα άπειρο) (μάλιστα μπορούμε να βρούμε άπειρα τέτοια σημεία). Έστω, λοιπόν $P = (a, b, 0) \notin A_0$. όμως $P \neq (0, 0, 0)$ και άρα χ.β.γ υποθέτουμε $b \neq 0$ και άρα $P = (c, 1, 0)$ Αυτό το σημείο θα μας δώσει την κλίση της ευθείας που ψάχνουμε. Ανεβαίνουμε λοιπόν στο $z = 1$. Θεωρούμε την οικογένεια ευθειών $L_\lambda = \{\lambda Y + \lambda c X - Z, \lambda \in k\}$. Τότε τομή με το επίπεδο $z = 1$ παίρνουμε ότι $L_\lambda = \begin{cases} \lambda Y + \lambda c X \\ z = 1 \end{cases} := l_\lambda$ Αυτές οι ευθείες στο $z = 1$ είναι όλες παράλληλες.



Σχήμα 4.10: Παράλληλές ευθείες που η κλίση τους δίνεται από το σημείο M

Προφανώς επειδή η οικογένεια αυτή περιλαμβάνει άπειρες ευθείες και το A_1 είναι πεπερασμένο, θα υπάρχει τουλάχιστον μία ευθεία (άπειρες) ώστε να μην τέμνει κανένα σημείο του A^1.

□

4.5 Πολυπροβολικός Χώρος

Θέλουμε να μετατρέψουμε το καρτεσιανό γινόμενο δύο ποικιλοτήτων σε ποικιλότητα. Αφού το $A^n \times A^m$ ταυτίζεται με το A^{n+m}, αυτό δεν είναι δύσκολο για αφφινικές ποικιλότητες. Τα πράγματα όμως δεν είναι τόσο απλά στην περίπτωση $P^n \times P^m$ καθώς ο χώρος αυτός δεν είναι ισόμορφος με τον P^{n+m}. Οι προσπάθειες είναι παρόμοιες με αυτές στις διαφορίσιμες πολλαπλότητες όπου ψάχνουμε τρόπους να εμβυθίσουμε καρτεσιανό γινόμενο πολλαπλοτήτων $M \times N$ διάστασης m και n αντίστοιχα σε μία μεγαλύτερη πολλαπλότητα S. Τα ερωτήματα που προκύπτουν είναι πόσο μεγάλη (σε διάσταση) χρειάζεται να είναι αυτή η πολλαπλότητα και με ποιο τρόπο (κατασκευαστικό) μπορούμε να την εμβυθίσουμε.

Περιληπτικά θα δούμε ένα αντίστοιχο παράδειγμα/άσκηση στους προβολικούς χώρους και θα προσπαθήσουμε να απαντήσουμε στα δύο αυτά ερωτήματα. Δεν είναι τυχαίο ότι η απάντηση είναι κοινή στις πολλαπλότητες και στους προβολικούς χώρους.

Πρόταση 4.16. *Για απλούστευση συμβολισμού, θεωρούμε $X_0, ..., X_n$ οι συντεταγμένες του P^n και $Y_0, ..., Y_m$ οι συντεταγμένες του P^m και $T_{00}, T_{01}, ..., T_{0m}, T_{10}, ..., T_{nm}$ συντεταγμένες του P^N όπου $N = (n+1)(m+1) - 1 = n + m + nm$.*

Ορίζουμε $S : P^n \times P^m \to P^N$ ως εξής : $S((x_0, ..., x_n), (y_0, ..., y_m)) = (x_0y_0, x_0y_1, ..., x_ny_m)$. Το S λέγεται Segre imbedding (εμβύθιση του Segre) του $P^n \times P^m$ στο P^{n+m+nm}.

1. *Να δείξετε ότι η S είναι καλά ορισμένη, 1-1 απεικόνιση.*

2. *Να δείξετε ότι αν W είναι αλγεβρικό υποσύνολο του P^N, τότε $S^{-1}(W)$ είναι αλγεβρικό στο $P^n \times P^m$*

3. *Έστω* $V = V(\{T_{ij}T_{kl} - T_{il}T_{kj} \quad |i,k = 0,...,n; j,l = 0,...,m\}) \subset P^N$. *Να δείξετε ότι* $S(P^n \times P^m) = V$. *Μάλιστα* $S(U_i \times U_j) = V \cap U_{ij}$, *όπου* $U_{ij} = \{(t) \quad |t_{ij} \neq 0\}$.

4. *Να δείξετε ότι το* V *είναι ποικιλότητα.*

Απόδειξη. 1. Για να δείξουμε ότι η S είναι καλά ορισμένο αρκεί να δείξομυε ότι $S((x_0,...,x_n)(y_0,...,y_m)) = S((\lambda x_0,...,\lambda x_n),(\mu y_0,...,\mu y_m)) \quad \forall \lambda,\mu \neq 0$ που με στοιχειώδεις πράξεις βλέπουμε ότι ισχύει.

1-1: Έστω $S((x_0,...,x_n)(y_0,...,y_m)) = S((z_0,...,z_n)(w_0,...,w_m))$, τότε αρκεί να δείξουμε ότι $(x_0,...,x_n) = (z_0,...,z_n)$ και $(y_0,...,y_m) = (w_0,...,w_m)$.
Έχουμε $(x_0y_0, x_0y_1, ..., x_ny_m) = (z_0w_0, z_0w_1, ..., z_nw_m)$, δηλαδή $x_iy_j = \lambda z_iw_j \forall i,j$. Έστω χ.β.γ ότι $x_0 \neq 0$. Τότε $x_0y_j = z_0w_j \Rightarrow y_j = \frac{z_0w_j}{x_0} \Rightarrow (y_1,...,y_m) = (\frac{z_0}{x_0}w_1,...,\frac{z_0}{x_0}w_m) = (w_1,...,w_m)$. Όμοια για τα x_i κι έχουμε το ζητούμενο.

2. Έστω $W \subset P^N$ αλγεβρικό $\Rightarrow W = V(I) = V(F_1,....,F_s)$, όπου F_i ομογενή στο $k[X_1,....,x_{n+1}]$
Έστω $I' = I^T = \{F^T | F \in I\} = \{F(X_0Y_0, X_0Y_1, ..., X_nY_m)\} \quad |F \in I$.
Τότε τα F^T είναι διομογενή αφού F ομογενές. Πράγματι στο $k[X_1,...,X_n]$ το F^T μπορεί να θεωρηθεί ως $F^T = F(a_1X_0, a_2X_0, ..., a_{N+1}X_{N+1})$ όπου $a_i \in k[Y_o,...,Y_m]$, άρα ομογενές και ομοίως για το $k[Y_0,...,Y_m]$

Θα δείξουμε ότι $S^{-1}(W) = V(I')$. Έστω $P = ((a_0,...,a_n)(b_0,...,b_m)) \in S^{-1}(W) \Rightarrow S(P) = (a_0b_0, a_0b_1, ..., a$
$W = V(I) \Rightarrow F(a_0b_0,....,a_nb_m) = 0 \forall F \in I$

Όμως $F^T(P) = F(X_0Y_0, X_0Y_1, ..., X_nY_m)(P) = F(a_0b_0, a_0b_1, ..., a_nb_m) = 0 \forall F \in I \Rightarrow P \in I^T \Rightarrow S^{-1}(W) \subseteq V(I')$.

Έστω $P = ((a_0,...,a_n)(b_0,...,b_m)) \in V(I') \Rightarrow F^T(P) = 0 \forall F \in I \Rightarrow F(a_0b_0,....,a_nb_m) = 0 \forall F \in I \Rightarrow S(P) = (a_0b_0,...,a_nb_m) \in V(I) \Rightarrow P \in S^{-1}(W)$ και άρα $S^{-1}(W) = V(I')$

3. $V = V(\{T_{ij}T_{kl} - T_{il}T_{kj} \quad |i,k = 0,...,n; j,l = 0,...,m\})$ Θέλουμε να δείξουμε ότι $S(P^n \times P^m) = V$

Έστω $P' \in S(P^n \times P^m) \Rightarrow \exists P \in P^n \times P^m : P' = S(P) \Rightarrow P' = (a_0b_0, a_0b_1, ..., a_nb_m)$ για κάποια $a_i, b_j \in k$.
Συνεπώς $(T_{ij}T_{kl} - T_{il}T_{kj})(P) = a_ib_ja_kb_l - a_ib_la_kb_j = 0 \Rightarrow P \in V$. Άρα $S(P^n \times P^m) \subseteq V$

Έστω $P' \in V, P' = (x_{00}, x_{01}, ..., x_{0m}, x_{10}, ..., x_{nm})$ $P' \in V \Rightarrow x_{ij}x_{kl} = x_{il}x_{kj}$.
Έστω χ.β.γ $x_{00} \neq 0$ και $A = (x_{00}, x_{10}, ..., x_{n0}) \in P^n$ και $B = (x_{00}, x_{01}, ..., x_{0m}) \in P^m$. Τότε με πράξεις καταλήγουμε ότι $P = S(A,B)$ και άρα $S(P^n \times P^m) = V$

$S(U_i \times U_j) = V \cap U_{ij}$, όπου $U_{ij} = \{(t)|t_{ij} \neq 0\}$. Πάλι με διπλό εγκλεισμό προκύπτει εύκολα ότι ισχύει.

4. Έστω $V = V_1 \cup V_2$ όπου V_1, V_2 αλγεβρικά. Συνεπώς $S^{-1}(V) = S^{-1}(V_1) \cup S^{-1}(V_2)$.
Από το (2) $S^{-1}(V_1), S^{-1}(V_2)$ είναι αλγεβρικά. Αφού S 1-1, άρα $S^{-1}(V_1), S^{-1}(V_2)$ είναι γνήσια υποσύνολα. Άρα $P^n \times P^m = S^{-1}(V_1) \cup S^{-1}(V_2)$, δηλαδή το $P^n \times P^m$ δεν είναι ανάγωγο που είναι άτοπο αφού εύκολα ελέγει κανείς ότι P^n ανάγωγο και P^m ανάγωγο $\Rightarrow P^n \times P^m$ ανάγωγο.

□

Η πρόταση αυτή μας δείχνει έναν πολύ σημαντικό κα χρήσιμο κατασκευαστικό τρόπο να εμβυθίσουμε το $P^n \times P^m$ σε έναν προβολικό χώρο μεγαλύτερης διάστασης. Δεν απαντάει όμως στο ερώτημα εάν αυτός είναι ο μικρότερος δυνατός προβολικός χώρος στον οποίο μπορούμε να το εμβυθίσουμε. Η απάντηση εν γένει είναι όχι αλλά δεν είναι καθόλου τετριμμένη.

Γενικά ισχύει το θεώρημα

Θεώρημα 4.2. *Πάνω από ένα αλγεβρικά κλειστό σώμα, οποιοδήποτε προβολική λεία ποικιλότητα διάστασης* n *μπορεί να εμβυθιστεί στο* P^{2n+1}.

Αυτό το αποτέλεσμα μπορεί να βρεθεί στο Shafarevich's Basic Algebraic Geometry, κεφάλαιο II, παρ. 5.4. [Sha96] Αυτή η εμβύθιση είναι ακριβής (sharp) δηλαδή για κάθε n μπορούμε να βρούμε λεία προβολική ποικιλότητα διάστασης n που να μη μπορεί να εμβυθιστεί στο P^{2n}. Η απόδειξη παρ΄ όλ΄ αυτά του θεωρήματος είναι υπαρξιακή και όχι κατασκευαστική, γεγονός που κάνει το Segre embedding αρκετά χρήσιμο. Παρατηρούμε, βέβαια ότι το $P^n \times P^m$ έχει διάσταση $n+m$ και για μεγάλα αρκετά n, m το $2(n+m)+1$ είναι αρκετά μικρότερο του $(n+1)(m+1)-1$.

Το ακριβές αντίστοιχο στις διαφορίσιμες πολλαπλότητες είναι το θεώρημα του Whitney . Δεν θα επιμείνουμε, όμως παραπάνω γιατί ήδη ξεφύγαμε από τα όρια της εργασίας αυτής.

Κεφάλαιο 5

Θεώρημα Bezout

Φτάσαμε στον κύριο στόχο της εργασίας. Αρχικά θα γενικεύσουμε όσες έννοιες αναφέραμε στο 3ο κεφάλαιο, στον προβολικό χώρο.

5.1 Προβολικές επίπεδες καμπύλες

Μία προβολική επίπεδη καμπύλη είναι μία υπερεπιφάνεια στον P^2, επιτρέποντας βέβαια πολλαπλούς παράγοντες. Δύο μη σταθερά, ομογενή πολυώνυμα $F, G \in k[X, Y, Z]$ είναι ισοδύναμα εάν υπάρχει μη σταθερό $\lambda \in k : F = \lambda G$. Μία προβολική επίπεδη καμπύλη λοιπόν είναι μία κλάση ισοδυναμίας από ομογενή πολυώνυμα. Ο βαθμός της καμπύλης, είναι ο βαθμός των ομογενών αυτών πολυωνύμων. Καμπύλες βαθμού 1, 2, 3 και 4 λέγονται ευθείες, κωνικές, κυβικές και τεταρτοβάθμιες αντίστοιχα. Όσους συμβολισμούς και συμβάσεις είχαμε κάνει στο 3ο κεφάλαιο ισχύουν όμοια και στον προβολικό χώρο κι έτσι γράφουμε πάλι για παράδειγμα $\mathcal{O}_P(F)$ αντί για $\mathcal{O}_P(V(F))$. Παρατηρείστε ότι εάν $P = (x, y, 1)$, τότε το $\mathcal{O}_P(F)$ είναι κανονικά ισόμορφο με το $\mathcal{O}_{(x,y)}(F_*)$, όπου $F_* = F(X, Y, 1)$ η αντίστοιχη αφφινική καμπύλη.

Στο κεφάλαιο 3 δείξαμε ότι η πολλαπλότητα ενός σημείου σε μία αφφινική καμπύλη εξαρτάται μόνο από τον τοπικό δακτύλιο της καμπύλης στο σημείο αυτό. Συνεπώς, εάν F μία προβολική επίπεδη καμπύλη και $P \in U_i (i = 1, 2, 3)$ μπορούμε να απομογενοποιήσουμε την F ως προς το X_i και να ορίσουμε την πολλαπλότητα της F στο σημείο P ως $m_P(F_*)$. Η πολλαπλότητα είναι ανεξάρτητη της επιλογής U_i και αναλλοίωτη μέσα από προβολική αλλαγή συντεταγμένων.

Ισχύει μία ανάλογη πρόταση για τα πολλαπλά σημεία:

Πρόταση 5.1. *Έστω F προβολική επίπεδη καμπύλη. Ένα σημείο P είναι πολλαπλό στην F αν-ν $F(P) = F_X(P) = F_Y(P) = F_Z(P)$.*

Απόδειξη. Ισχύει $m_P(F) = m_P(F_*)$ και άρα εάν P είναι πολλαπλό, έχουμε ότι $(F_*)_X(P) = (F_*)_Y(P) = 0$. Εύκολα επίσης βλέπουμε ότι $(F_*)_X = (F_X)_*$ και άρα $(F_X)_*(P) = 0$.

Έστω χ.β.γ ότι $P = (0, 0, 1)$ (αν όχι κάνουμε προβολική αλλαγή συντεταγμένων). Τότε παρατηρούμε ότι $(F_X)_*(0, 0) = (F_X)(0, 0, 1) = F_X(P)$. Όμως $(F_X)_*(0, 0) = 0$ και άρα καταλήγουμε ότι $F_X(P) = 0$. Όμοια για τα F_Y, F_Z και καταλήγουμε στο ζητούμενο.

□

Για μία πεπερασμένη συλλογή σημείων $P_1, ..., P_n \in P^2$, μπορούμε πάντα να βρούμε ευθεία L που δεν περνάει από κανένα από αυτά τα σημεία (προτ. 4.15). Εάν η F είναι καμπύλη βαθμού d, τότε ορίζουμε $F_* = F/L^d \in k(P^2)$. Το F_* εξαρτάται από την L, αλλά εάν η L' ήταν μία άλλη επιλογή, τότε $F/L'^d = (L/L')^d F_*$ και L/L' είναι μονάδα στο $\mathcal{O}_{P_i}(P^2)$. Παρατηρείστει βέβαια, ότι μπορούμε πάντα να βρούμε προβολική αλλαγή συντεταγμένων τ.ω η ευθεία L να γίνεται η ευθεία Z στο άπειρο. Άρα μέσω της φυσικής ταύτισης του $k(A^2)$ με το $k(P^2)$, αυτή η F_* είναι ίδια με την παλιά $F_* = F(X, Y, 1)$.

Εάν το P είναι απλό σημείο στην F και F ανάγωγη, τότε το $\mathcal{O}_P(F)$ είναι Δ.Δ.Ε. Με ord_P^F θα συμβολίζουμε την αντίστοιχη συνάρτηση τάξης στο $k(F)$. Εάν το G είναι ομογενές στο $k[X,Y,Z]$, και $G_* \in \mathcal{O}_P(P^2)$ ορίζεται όπως στην προηγούμενη παράγραφο, και $\overline{G_*}$ η εικόνα του G_* στο $\mathcal{O}_P(F)$, τότε ορίζουμε $ord_P^F(G) := ord_P^F(\overline{G_*})$.

Έστω F, G επίπεδες καμπύλες και $P \in P^2$. Ορίζουμε $i_P(F,G) := dim_k(\mathcal{O}_P(P^2)/(F_*, G_*))$. Ο ορισμός αυτός είναι ανεξάρτητος της επιλογής που ορίστηκαν τα F_*, G_* και ικανοποιεί τις γνωστές 8 ιδιότητες (παρ. 3.3). Παρ΄ όλ΄ αυτά, στην (3) η T προφανώς θα πρέπει να είναι προβολική αλλαγή συντεταγμένων και όχι αφφινική, και στην (7), το A πρέπει να είναι ομογενές βαθμού $\deg(A) = \deg(G) - \deg(F)$.

Ορίζουμε μία ευθεία L να είναι εφαπτόμενη σε μία καμπύλη F στο P αν $i_P(F,L) > m_P(F)$ (προτ. 3.6). Το P λέγεται κανονικό/σύνηθες πολλαπλό σημείο της F εάν η F έχει $m_P(F)$ σε πλήθος εφαπτόμενες ευθείες.

Εφαρμογή 5.1. *Να δείξετε ότι οι παρακάτω καμπύλες είναι ανάγωγες. Να βρείτε τα πολλαπλά σημεία καθώς και τις πολλαπλότητες και τις εφαπτομένες των σημείων αυτών.*

1. $F = XY^4 + YZ^4 + XZ^4$
2. $F = X^2Y^3 + X^2Z^3 + Y^2Z^3$

Απόδειξη. Από το κεφάλαιο 4.3 έχουμε ότι εάν $V \subset P^n$ και κανένας παράγοντας δεν κείται ή δεν περιέχει το H_∞, τότε το $V_* \subsetneq A^n$ και $(V_*)^* = V$. Αλγεβρικά αυτό σημαίνει ότι αν F ομογενές και $V = V(F)$, τότε εάν $Z \nmid F \Rightarrow (V_*)^* = V$.

Από πρόταση 4.13 έχουμε ότι εάν V_* ανάγωγο στο A^n, τότε $(V_*)^*$ ανάγωγο στο P^n. Συνεπώς αρκεί να δείξουμε ότι το F_* είναι ανάγωγο στο $k[X,Y]$ (αφού τότε $V_* = v(F_*)$ ανάγωγο).

1. $F = XY^4 + YZ^4 + XZ^4$
   $F_* = XY^4 + Y + X = F_1 + F_5$.
   Έστω F_* όχι ανάγωγο, δηλαδή $F = GH \Rightarrow G = G_0$+υψηλότεροι όροι... και $H = H_1$+ υψηλότεροι όροι... Τότε $G_0 = 1, H_1 = X + Y$ κι εύκολα καταλήγουμε σε άτοπο, άρα F_* όντως ανάγωγο και άρα $V(F_*)$ ανάγωγο, συνεπώς $V(F_*)^*$ ανάγωγο και $V(F*)^* = V(F_*^*)$

   Για τα πολλαπλά σημεία χρησιμοποιούμε την πρόταση 5.1. Έχουμε :
   $F_X = Y^4 + Z^4, \quad F_y = 4XY^3 + Z^4, \quad F_Z = XZ^3 + 4YZ^3 = 4Z^3(X+Y)$.
   Λύνουμε $F_X = F_Y = F_Z = F(P) = 0$ και με πράξεις καταλήγουμε ότι $(x,y,z) = (0,0,0) \notin P^2$ και άρα η F δεν έχει πολλαπλά σημεία.

2. $F = X^2Y^3 + X^2Z^3 + Y^2Z^3$
   $F_X = 2XY^3 + 2XZ^3 = 2X(Y^3 + Z^3)$
   $F_Y = 3X^2Y^2 + 2YZ^3 = Y(2Z^3 + 3X^2Y)$
   $F_Z = 3X^2Z^2 + 3Y^2Z^2 = 3Z^2(X^2 + Y^2)$
   $F_* = X^2Y^3 + 3Y^2Z^2 = GH$

   Με πράξεις όπως πριν προκύπτει ότι F_* ανάγωγο και άρα $V(F)$ ανάγωγο. Για τα πολλαπλά λύνουμε $F = F_X = F_Y = F_Z = 0$ και με πράξεις βρίσκουμε ότι

   $$(x,y,z) = \{(1,0,0),(0,1,0),(0,0,1)\}$$

   Για $P = (1,0,0)$:
   $m_P(F) = m_P(F_*)$. Διαλέγουμε να κάνουμε απομογενοποίηση στο X, δηλαδή $m_P(F) = m_{(0,0)}(F(1,Y,Z))$
   $F(1,Y,Z) = Y^3 + Z^3 + Y^2Z^3 = F_3 + F_5$, και άρα $m_P(F_*) = 3$.
   Οι εφαπτόμενες ευθείες: $F_3 = Y^3 + Z^3 = (Y+Z)(Y^2 - ZY + Z^2) = (Y+Z)(Y - \omega Z)(Y - \bar{\omega} Z)$ και άρα $L_1 = Y + Z, L_2 = Y - \omega Z, L_3 = (Y - \bar{\omega} Z)$.

Για $P = (0, 1, 0)$:
$m_P(F) = m_{(0,0)}(F(X, 1, Y))$, όπου $F(X, 1, Y) = X^2 + X^2Z^3 + Z^3$ και άρα $m_{(0,0)}(F_*) = 2$. $L = X$ διπλή εφαπτομένη.

Για $P = (0, 0, 1)$:
$m_P(F) = m_{(0,0)}(F(X, Y, 1))$, όπου $F(X, Y, 1) = X^2Y^3+X^2+Y^2$. Άρα $m_P(F) = 2$ και $F_2 = X^2+Y^2 = (X + iY)(X - iY)$ και άρα $L_1 = X + iY, L_2 = X - iY$ οι εφαπτόμενες ευθείες.

□

Για την επόμενη πρόταση/άσκηση θα χρειαστούμε το θεώρημα του Euler :

Θεώρημα 5.1 (θεώρημα του Euler). *Αν F ομογενές βαθμού m στο $R[X_1, ..., X_n]$, όπου R αντιμεταθετικό δακτύλιος, τότε $mF = \sum_{i=1}^{n} X_iF_{X_i}$*

Πρόταση 5.2. *Έστω P απλό σημείο στην F. Τότε ότι η εφαπτόμενη ευθεία της F στο P είναι $F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0$*

Απόδειξη. L εφαπτόμενη στην $F \Leftrightarrow i_P(F, L) > m_P(F)$. Έστω $L = aX + bY + cZ$ και $P = (x, y, 1)$ (Προφανώς απαιτούμε $ax + by + c = 0$)
Τότε $i_P(F, L) = I_{(x,y)}(F_*, L_*) = i_{(x,y)}(F_*, aX + bY + c)$.
Το P είναι απλό σημείο στην F αν-ν $P = (x, y)$ απλό σημείο στην $F_* \Leftrightarrow L_* = (F_*)_X(P)(X-x)+(F_*)_Y(P)(Y-y) = F_X(P)(X - x) + F_Y(P)(Y - y)$ η εφαπτόμενη ευθεία στην F_*
Συνεπώς

$$(L_*)^* = F_X(P)(X - xZ) + F_Y(P)(Y - yZ) = F_X(P)X + F_Y(P)Y - (xF_X(P) + yF_Y(P))Z \quad (1)$$

Όμως από το θεώρημα του Euler , αφού F ομογενές, άρα $F_XX + F_YY + F_ZZ = mF$ όπου $m = degF$
Και άρα $F_X(P)x + F_Y(P)y + F_Z(P)1 = 0$, άρα $(1) \Rightarrow F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0$

□

Πρόταση 5.3. *Δύο επίπεδες καμπύλες χωρίς κοινούς παράγοντες τέμνονται σε πεπερασμένο αριθμό σημείων.*

Απόδειξη. Έστω F, G ομογενή και $V(F), V(G)$ οι αντίστοιχες επίπεδες καμπύλες. Αφού οι F, G δεν έχουν κοινούς παράγοντες, άρα και οι F_*, G_* δεν έχουν κοινούς παράγοντες (προφανές). Άρα $V(F_*) \cap V(G_*) =$ πεπερασμένο $= \{P_1, ..., P_s\} \Rightarrow V(F_*, G_*) =$ πεπερασμένο $\Rightarrow V(F) \cap V(G) \cap V(U_3) =$ πεπερασμένο.
Όμοια $V(F) \cap V(G) \cap V(U_2) =$ πεπερασμένο και $V(F) \cap V(G) \cap V(U_1) =$ πεπερασμένο.
Άρα $V(F) \cap V(G)$ πεπερασμένο.

□

Πρόταση 5.4. *Έστω F ανάγωγη καμπύλη.*

1. *Να δείξετε ότι F_X, F_Y ή $F_z \neq 0$.*

2. *Να δείξετε ότι η F έχει πεπερασμένα σε αριθμό πολλαπλά σημεία.*

Απόδειξη. (1) προφανές
(2) Από την πρόταση 5.1 το P πολλαπλό αν-ν $F_X(P) = F_Y(P) = F_Z(P)$
Από το (1) έστω χ.β.γ $F_X \neq 0$. Αν F_X έχει κοινούς παράγοντες με την F τότε η F όχι ανάγωγη. Άρα από την προηγούμενη πρόταση έχουμε ότι $V(F, F_X)$ πεπερασμένο.

□

Πρόταση 5.5. *Έστω F ανάγωγο κωνικό, $P = (0,1,0)$ απλό σημείο στην F και $Z = 0$ η εφαπτόμενη ευθεία στην F στο P.*

1. *Τότε $F = aYZ - BX^2 - cXZ - dZ^2, \quad a, b \neq 0$. Υπάρχει προβολική αλλαγή συντεταγμένων T τ.ω $F^T = YZ - X^2 - c'XZ - d'Z^2$. Επιπλέον υπάρχει T' τ.ω $(F^T)^{T'} = YZ - X^2$*

2. *Ως προς την προβολική ισοδυναμία, υπάρχει μοναδικός κώνος. Κάθε ανάγωγο κωνικό πολυώνυμο είναι μη ιδιάζον.*

Απόδειξη. F κωνικό, δηλαδή F ομογενές και $\deg F = 2$. Άρα $F = aYZ - bX^2 - cXZ - dZ^2 - eY^2 - gXY$.
$P \in F \Rightarrow e = 0$
P απλό $\overset{5.2}{\Rightarrow} L = F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0$. Όμως Z η εφαπτομένη και άρα $F_X(P) = F_Y(P) = 0, F_Z(P) = 1$. Συνεπώς $F_X(P) = 0 \Rightarrow g = 0$ και $F_Z(P) = 1 \Rightarrow a \neq 0$.
F ανάγωγο $\Rightarrow b \neq 0$.
Άρα $F = aYZ - bX^2 - cXZ - dZ^2$.
Θεωρούμε $T = (\frac{1}{\sqrt{b}}X, \frac{1}{a}Y, Z)$ και τότε $F^T = YZ - X^2 - c'XZ - d'Z^2$.

Θεωρούμε, τέλος, $T' = (X, Y + c'X + d'Z, Z)$. Τότε $(F^T)^{T'} = YZ - X^2$

Έστω F ανάγωγος κώνος.

$$F = a_1X^2 + a_2Y^2 + a_3Z^3 + a_4XY + a_5XZ + a_6YZ$$

$F_X = 2a_1X + a_4Y + a_5z$
$F_Y = 2a_2Y + a_4X + a_6Z$
$F_Z = 2a_3Z + a_5X + a_6Y$
Τα F_{X_i} είναι γραμμική (ή μηδέν). Σίγουρα, όμως, υπάρχει X_i τ.ω F_{X_i} γραμμικό. Έστω χ.β.γ ότι $F_X \neq 0$ και $P \in F$.
Αν το P σημείο της F και όχι απλό, τότε P πολλαπλό και άρα από την πρότ. 5.2 έχουμε $F_X(P) = F_Y(P) = F_Z(P)$. Όμως υπάρχουν πεπερασμένα μόνο πολλαπλά σημεία (προτ. 5.4), ενώ η F έχει άπειρα σημεία, και συνεπώς συμπεραίνουμε ότι υπάρχει τουλάχιστον ένα απλό (άπειρα μάλιστα) σημείο $P \in F$. Έστω χ.β.γ $P = (a, 1, c) \in U_2$ και έστω L η εφαπτόμενη ευθεία.

Από την ... υπάρχει Τ προβολική αλλαγή συντεταγμένων τ.ω $P^T = (0,1,0)$ και $L^T = Z$. Άρα από το (1) έχουμε τελειώσει. □

Με όμοιο τρόπο δείχνουμε ότι υπάρχει μοναδικό ανάγωγο κυβικό πολυώνυμο (ως προς την προβολική ισοδυναμία).

5.2 Θεώρημα Bezout

Όσα έχουμε μελετήσει σε αυτή την εργασία καταλήγουν στο θεώρημα του Bezout .

Θεώρημα 5.2 (Θεώρημα Bezout). *Έστω F, G προβολικές επίπεδες καμπύλες βαθμού m και n αντίστοιχα. Υποθέτουμε ότι F, G δεν έχουν κοινούς παράγοντες. Τότε*

$$\sum_P i_P(F, G) = mn$$

Με άλλα λόγια, δύο καμπύλες (στον προβολικό χώρο), βαθμού m και n αντίστοιχα, τέμνονται σε mn σημεία, μετρούμενης και της πολλαπλότητας

Απόδειξη. Αφού $F \cap G$ είναι πεπερασμένο (προτ. 5.3), μπορούμε νε υποθέσουμε, χρησιμοποιώντας προβολική αλλαγή συντεταγμένων άμα χρειαστεί, ότι κανένα από τα σημεία του $F \cap G$ ανήκει στην ευθεία στο άπειρο στο $Z = 0$.

Τότε από την 9η ιδιότητα για τον αριθμό τομής, έχουμε ότι

$$\sum_P i_P(F,G) = \sum_P i_P(F_*, G_*) = \dim_k k[X,Y]/(F_*, G*)$$

. Θέτουμε $\Gamma_* = k[X,Y]/(F_*, G_*)$ και $\Gamma = k[X,Y,Z]/(F,G), R = k[X,Y,Z]$ και Γ_d (αντ. R_d) τον δ.χ των ομογενών πολυωνύμων βαθμού d στο Γ (αντ. R) (το ότι αποτελεί δ.χ είναι προφανές ελέγχοντας μία μία τις ιδιότητες). Το θεώρημα θα αποδειχτεί εάν καταφέρουμε να δείξουμε ότι $\dim \Gamma_* = \dim \Gamma_d = mn$ για αρκετά μεγάλο d .

Βήμα 1: Θα δείξουμε ότι $\dim \Gamma_d = mn$ για κάθε $d \geq m+n$.

Έστω $\pi : R \to \Gamma$ η φυσική απεικόνιση, $\phi : R \times R \to R$, που ορίζεται από τη σχέση $\phi(A,B) = AF + BG$ και $\psi : R \to R \times R$ που ορίζεται από $\psi(C) = (GC, -FC)$. Χρησιμοποιώντας το γεγονός ότι τα F, G δεν έχουν κοινούς παράγοντες, εύκολα ελέγχουμε ότι η παρακάτω ακολουθία :

$$0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\phi} R \xrightarrow{\pi} \Gamma \longrightarrow 0$$

είναι ακριβής.
Εάν περιορίσουμε τις απεικονίσεις αυτές σε ομογενή πολυώνυμα διαφόρων βαθμών, παίρνουμε την επόμενη ακριβή ακολουθία:

$$0 \longrightarrow R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\phi} R_d \xrightarrow{\pi} \Gamma_d \longrightarrow 0$$

Αφού όμως $\dim R_d = \dfrac{(d+1)(d+2)}{2}$ συμπεραίνουμε με απλές πράξεις ότι $\dim \Gamma_d = mn$ αν $d \geq m+n$

Βήμα 2: Η απεικόνιση $\alpha : \Gamma \to \Gamma \quad \alpha(\overline{H} = \overline{ZH})$ (όπου με μπάρα υποδηλώνουμε την εικόνα μοδίω (F,G)) είναι 1-1.

Αρκεί να δείξουμε ότι εάν $\alpha(\overline{H}) = 0$ τότε $\overline{H} = 0$. Δηλαδή εάν $ZH = AF + BG$, τότε $H = A'F + B'G$. Για $J \in k[X,Y,Z]$ θα συμβολίζουμε (παροδικά) με J_0 το $J(X,Y,0)$. Αφού F, G και Z δεν έχουν κοινά σημεία μηδενισμού (έτσι τα κατασκευάσαμε εξαρχής), άρα το F_0, G_0 είναι μεταξύ τους πρώτα ομογενή πολυώνυμα στο $k[X,Y]$.

Αν $ZH = AF + BG$, τότε $A_0F_0 = -B_0G_0$ και άρα $B_0 = F_0C$ και $A_0 = -G_0C$ για κάποιο $C \in k[X,Y]$.

Έστω $A_1 = A + CG, B_1 = B - CF$. Αφού $(A_1)_0 = (B_1)_0 = 0$ έχουμε ότι $A_1 = ZA', B_1 = ZB'$ για κάποια A', B', και αφού $ZH = A_1F + B_1G$, συμπεραίνουμε ότι $H = A'F + B'G$, όπως θέλαμε.

Βήμα 3: Έστω d αρκετά μεγάλο, δηλαδή $d \geq m+n$. Το Γ_d έχει διάσταση mn άρα μπορούμε να βρούμε $A_1, ..., A_{mn} \in R_d$, των οποίων η εικόνα στο Γ_d αποτελεί βάση του Γ_d. Θέτουμε $A_{i*} = A_i(X,Y,1) \in k[X,Y]$ και a_i η εικόνα του A_{i*} στο Γ_*. Αρκεί να δείξουμε ότι τα $a_1, ..., a_{mn}$ αποτελούν βάση του Γ_*

Αρχικά παρατηρούμε ότι ότι η απεικόνιση α του δεύτερου βήματος περιορίζεται σε ισομορφισμό από το Γ_d στο Γ_{d+1}, για $d \geq m+n$, αφού μία 1-1 απεικόνιση μεταξύ διανυσματικών χώρων ίδιας διάστασης είναι ισομορφισμός. Συνεπώς, οι εικόνες των $Z^rA_1, ..., Z^rA_{mn}$ αποτελούν βάση του Γ_{d+r} για κάθε $r \geq 0$.

Τα a_i παράγουν το Γ_*: Εάν $h = \bar{H} \in \Gamma_*, H \in k[X,Y]$, το Z^NH^* είναι ομογενές βαθμού $d+r$ για κατάλληλο N και άρα $Z^NH^* = \sum i = 1^m n\lambda_i Z^r A_i + BF + CG$ για $\lambda_i \in k, B, C \in k[X,Y,Z]$.
Τότε $H = (Z^NH^*)_* = \sum \lambda_i A_{i*} + B_*F_* + C_*G_*$ και συνεπώς $h = \sum \lambda_i a_i$ όπως θέλαμε.

Τα a_i είναι ανεξάρτητα: Έστω $\sum \lambda_i a_i = 0$, τότε $\sum \lambda_i A_{i*} = BF_* + CG_*$. Συνεπώς από πρόταση 4.1 έχουμε ότι $Z^r \sum \lambda_i A_i = Z^s B^* F + Z^t C^* G$ για κατάλληλα r, s, t. Όμως, τότε $\sum \lambda_i \overline{Z^r A_i} = 0$ στο Γ_{d+r}, και τα $\overline{Z^r A_i}$ αποτελούν βάση και άρα κάθε $\lambda_i = 0$, που ολοκληρώνει την απόδειξη.

□

Συνδιάζοντας την ιδιότητα 5 από τους αριθμούς τομής μαζί με το θεώρημα Bezout συμπεραίνουμε αμέσως και τα εξής λήμματα:

Λήμμα 5.1. *Αν F, G δεν έχουν κοινούς παράγοντές, τότε $\sum_P m_P(F) m_P(G) \leq \deg(F)\deg(G)$.*

Λήμμα 5.2. *Αν F, G τέμνονται σε mn διακεκριμένα σημεία, $m = \deg(F), n = deg(G)$, τότε όλα αυτά τα σημεία είναι απλά στην F και G.*

Λήμμα 5.3. *Αν δύο καμπύλες βαθμού m και n τέμνονται σε περισσότερα από mn σημεία, τότε έχουν αναγκαστικά κοινό παράγοντα.*

Bibliography

[AM69] Michael Francis Atiyah and I. G MacDonald. *Introduction to commutative algebra.* 1969.

[Mum70] David Mumford. *Algebraic Geometry I, Complex Projective Varieties.* 1970.

[Har77] Robin Hartshorne. *Algebraic Geometry.* 1977.

[Ful89] William Fulton. *Algebraic curves - an introduction to algebraic geometry.* 1989. URL: `http://xahlee.info/math/i/algebraic_geometry_by_william_fulton_73219.pdf`.

[Eis95] D. Eisenbud. *Commutative Algebra with a view toward Algebraic Geometry.* 1995.

[Sha96] Igor R. Shafarevich. *Basic Algebraic Geometry 2.* 1996.

[CLO08] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* 2008.

[Har] Charalambous Hara. *Introduction to Commutative Algebra.* Greek. URL: `http://users.auth.gr/~hara/Books-Notes/commutative.pdf`.

Ευρετήριο

$R-module$ ομομορφισμός, 41
ΔΔΕ, 34
ακριβής ακολουθία, 41
αλγεβρικό σύνολο, 10
ανάγωγο, 16
αναλύσιμο, 16
αφφινική αλλαγή συντεταγμένων, 29
αφφινική ευθεία, 10, 31
αφφινική ποικιλότητα, 17
αφφινική ψευδοποικιλότητα, 19
αφφινικό επίπεδο, 10
απλό σημείο, 46
δακτύλιος συντεταγμένων, 25
διάσταση γραμμικής ποικιλότητας, 30
εφαπτόμενη ευθεία, 46
γραμμική υποποικιλότητα, 30
ομογενές δακτύλιος συντεταγμένων, 62
ομογενές σώμα συναρτήσεων, 63
ομοιομορφοποιητής, 35
πόλος της f, 32
πολλαπλό, 46
πολυωνυμική απεικόνιση, 27
πολυωνυμική συνάρτηση, 25
προβολική αλλαγή συντεταγμένων, 63
προβολική ποικιλότητα, 61
προβολικός χώρος, 59
ρητή συνάρτηση, 32
σώμα ρητών συναρτήσεων, 32
σημείο καμπής, 50
σημείο υψηλότερης καμπής, 50
συνάρτηση τάξης, 35
τοπικός δακτύλιος του V στο P, 32
τοπολογία, 9
υπερεπίπεδο, 10
υπερεπιφάνεια, 10
Noetherian δακτύλιος, 11
Noetherian τοπολογικός χώρος, 19
R-module , 41
Segre embedding , 69
χαρακτηριστική καμπύλη , 46