2ο Φυλλάδιο Ασκήσεων - Θεωρία Galois

Αναστάσιος Φράγκος: ΑΜ 1112201900239 Πέμπτη, 14 Απριλίου 2022

Συμβολισμοί - Παρατηρήσεις

1. $[x^k]_f$: Είναι ο συντελεστής του x^k στο πολυώνυμο f. **2.** Έστω C και D δύο σχήματα στο επίπεδο τα οποία έχουν το πολύ 1 σημείο τομής. Συμβολίζουμε με $C \cap D$ το σημείο τομής τους (εάν αυτό υπάρχει). Να σημειωθεί ότι αυτή η τομή δεν είναι η συνολοθεωρητική τομή. **3.** Εάν $A \neq B$ είναι δύο σημεία, θα συμβολίζουμε με $\overrightarrow{AB}$ την ημιευθεία με αρχή το A που διέρχεται από το B και με $\overleftrightarrow{AB}$ την ευθεία από τα A, B.

Άσκηση 1 Δείξτε ότι $\mathbb{Q}(\pi) \cap \overline{\mathbb{Q}} = \mathbb{Q}$ ■

Λύση: Για τη λύση της άσκησης αυτής αρκεί να αποδειχθεί ο εγκλεισμός $\mathbb{Q}(\pi) \cap \overline{\mathbb{Q}} \subseteq \mathbb{Q}$, μιας και ο άλλος είναι άμεση συνέπεια του ότι $\mathbb{Q} \subseteq \mathbb{Q}(\pi)$ και $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$.

Υποθέτουμε προς άτοπο ότι υπάρχει ένας αριθμός $c \in \mathbb{Q}(\pi) \cap \overline{\mathbb{Q}}$ ο οποίος δεν ανήκει στο $\mathbb{Q}$. Αυτός ο αριθμός c θα λαμβάνει δύο μορφές, οι οποίες είναι οι ακόλουθες:

$$c = \frac{f(\pi)}{g(\pi)},\ f, g \in \mathbb{Q}[x],\ \text{επειδή } c \in \mathbb{Q}(\pi)$$

κι επιπλέον:

$$h(c) = 0 \text{ για κάποιο } h \in \mathbb{Q},\ \text{αφού } c \in \overline{\mathbb{Q}}$$

Θα πρέπει λοιπόν να αληθεύει η σχέση:

$$h\left(\frac{f(\pi)}{g(\pi)}\right) = 0$$

για κάποια πολυώνυμα f, g, h με ρητούς συντελεστές. Ισοδύναμα, κανείς μπορεί να παραστήσει την προηγούμενη σχέση χρησιμοποιώντας τον **Συμβολισμό 1**:

$$\sum_{k=0}^{\deg h} [x^k]_h \cdot \left(\frac{f(\pi)}{g(\pi)}\right) = 0 \Rightarrow \sum_{k=0}^{\deg h} [x^k]_h \cdot g(\pi)^{\deg h - k} f(\pi)^k = 0$$

Θεωρούμε τώρα το πολυώνυμο ρητών συντελεστών:

$$P(x) = \sum_{k=0}^{\deg h} [x^k]_h \cdot g(x)^{\deg h - k} f(x)^k = 0$$

και παρατηρούμε ότι αυτό έχει ρίζα το π (κατ' επέκταση, $\pi \in \overline{\mathbb{Q}}$). Αυτό είναι άτοπο, αφού ο Lindemann έδειξε ότι το π είναι υπερβατικός.

Αναγκαστικά λοιπόν, εάν ένας αριθμός c βρίσκεται στην τομή $\mathbb{Q}(\pi) \cap \overline{\mathbb{Q}}$, τότε ανήκει στο $\mathbb{Q}$ - αυτό αποδεικνύει τον εγκλεισμό $\mathbb{Q}(\pi) \cap \overline{\mathbb{Q}} \subseteq \mathbb{Q}$.

□

Άσκηση 2 Θεωρούμε τρία μη συνευθειακά κατασκευάσιμα σημεία στο επίπεδο και μια από τις οριζόμενες γωνίες. Δείξτε ότι η διχοτόμηση της γωνίας αυτής στα πλαίσια της Ευκλείδειας Γεωμετρίας επιτυγχάνεται με τις δύο διαδικασίες που είδαμε στο μάθημα ('κανόνας' και 'διαβήτης'). Με βάση αυτό, δείξτε ότι ο θετικός πραγματικός αριθμός $\cos 80°$ δεν είναι κατασκευάσιμος. ■

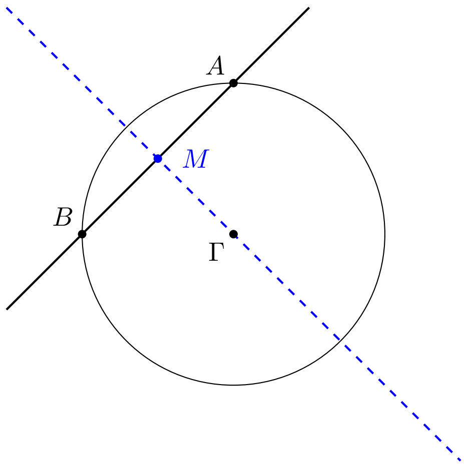
Λήμμα 2.1: *Εάν δύο αριθμοί είναι κατασκευάσιμοι, τότε το γινόμενο αυτών είναι αριθμός κατασκευάσιμος.*

Απόδειξη: Μπορείτε να βρείτε μια απόδειξη στον ακόλουθο σύνδεσμο:

http://users.uoa.gr/ sma1900239/files/others/gnt.pdf, στη σελίδα 16

(μην δώσετε βέβαια ιδιαίτερη σημασία στα υπόλοιπα - δεν είναι καλογραμμένα). Ένα κύριο σημείο το οποίο δεν εξηγείται στο εν λόγω έγγραφο είναι πώς κατασκευάζεται παράλληλη σε μια ευθεία από ένα σημείο. Ουσιαστικά γι'αυτό αρκεί να φερθεί κάθετος από το σημείο στην ευθεία, κι έπειτα μια κάθετη ευθεία προς την προηγούμενη κάθετο, από το σημείο αυτό. Χρειάζεται λοιπόν να αποδειχθεί ότι από τυχαίο σημείο μπορεί να φερθεί κάθετος σε ευθεία που δεν περιέχει το σημείο (φυσικά, δεδομένου ότι γνωρίζουμε πώς μπορούμε να φέρουμε μεσοκαθέτους - αυτό είναι κάτι που χρησιμοποιείται για να φέρουμε τόσο την πρώτη κάθετο, όσο και τη δεύτερη).

Βήμα Ι: Έστω Γ ένα σημείο, ε μια ευθεία που δεν το περιέχει και A που κείται επί της ε. Χαράσουμε κύκλο με κέντρο Γ και ακτίνα A, και θεωρούμε B το σημείο τομής του κύκλου με την ευθεία.



Βήμα ΙΙ: Φέρουμε τη μεσοκάθετο $\underleftrightarrow{M\Gamma}$ του AB και παρατηρούμε ότι αυτή είναι η ζητούμενη κάθετος.

$\triangle$

Λήμμα 2.2: *Εάν ένας (μη μηδενικός) αριθμός είναι κατασκευάσιμος, τότε ο αντίστροφος αυτού είναι επίσης κατασκευάσιμος*

<u>*Απόδειξη:*</u> Μπορείτε να βρείτε μια απόδειξη στον ακόλουθο σύνδεσμο:

http://users.uoa.gr/ sma1900239/files/geometry/hyper.pdf, στη σελίδα 62

ή στον:

http://users.uoa.gr/ sma1900239/files/others/gnt.pdf, στη σελίδα 17

$\triangle$

Άμεσο πόρισμα: *Το πηλίκο δύο μη μηδενικών κατασκευάσιμων αριθμών είναι αριθμός κατασκευάσιμος.*

Λήμμα 2.3: *Μια γωνία θ είναι κατασκευάσιμη εάν και μόνο αν το συνημίτονο αυτής $\cos\theta$ είναι κατασκευάσιμο.*

<u>*Απόδειξη:*</u> Αρκεί να εξετάσουμε την ισοδυναμία για γωνίες θ μεταξύ του 0 και του π.

($\Rightarrow$) Θεωρούμε X, O, Y τρία σημεία τα οποία σχηματίζουν γωνία $\theta = \widehat{XOY}$. Από το σημείο X φέρουμε κάθετο μ προς την ημιευθεία $\underrightarrow{OY}$ και θεωρούμε $M = \mu \cap \underrightarrow{OY}$ το σημείο τομής της καθέτου με την ημιευθεία. Τα ευθύγραμμα τμήματα XO, MO είναι κατασκευάσιμα, οπότε και τα μήκη τους $||XO||$, $||MO||$ είναι κατασκευάσιμοι αριθμοί. Από το **Άμεσο πόρισμα**, ο λόγος $\cos\theta = \dfrac{||MO||}{||XO||}$ είναι κατασκευάσιμος αριθμός.

($\Leftarrow$) Θεωρούμε OM ένα ευθύγραμμο τμήμα μήκους $\cos\theta$. Φέρουμε κάθετο μ από το M προς την ημιευθεία $\underrightarrow{OM}$ και από το O κύκλο C ακτίνας 1. Θεωρούμε εν τέλει X το σημείο τομής του κύκλου C με την κάθετο μ και παρατηρούμε ότι $\widehat{XOM} = \theta$. Επομένως η θ είναι κατασκευάσιμη.

$\triangle$

Λήμμα 2.4: *Ο αριθμός $\cos 20°$ δεν είναι κατασκευάσιμος.*

<u>*Απόδειξη:*</u> Η γωνία των $60°$ είναι κατασκευάσιμη, αφού είναι εσωτερική γωνία του κανονικού εξαγώνου. Εάν η γωνία των $20°$ είναι κατασκευάσιμη, χρησιμοποιώντας την ταυτότητα $\cos(3\theta) = 4\cos^3(\theta) - 2\cos(\theta)$ για $\theta = 20°$, θα πρέπει το πολυώνυμο:

$$P(x) = 2 \cdot \left(4x^3 - 3x - \frac{1}{2}\right) = 8x^3 - 6x + 1$$

να έχει ρίζα το $\cos 20°$. Επειδή το P είναι ανάγωγο υπεράνω του $\mathbb{Q}$, ο βαθμός $[\mathbb{Q}(\cos 20°) : \mathbb{Q}]$ είναι ακριβώς ο βαθμός του πολυωνύμου, δηλαδή 3.

Ο βαθμός αυτός είναι που θα μας δώσει το άτοπο, αφού μέσω διαδοχικών κατασκευών 'κανόνα' και 'διαβήτη' οι βαθμοί επέκτασης είτε διπλασιάζονται είτε μένουν αναλλοίωτοι, λόγω του ότι η τομή δύο στοιχείων της οικογένειας των ευθειών και κύκλων εκφράζεται το πολύ από δευτεροβάθμια πολυώνυμα. Κατ' επέκταση, ο βαθμός $[\mathbb{Q}(\cos 20°) : \mathbb{Q}]$ θα έπρεπε να ήταν 1 ή άρτιος.

$\triangle$

Λύση: Αρκεί να δείξουμε ότι η διχοτόμιση μιας γωνίας επιτυγχάνεται με 'κανόνα' και 'διαβήτη'. Εάν το $\cos 80°$ ήταν κατασκευάσιμος αριθμός, με δύο διαδοχικές διχοτομίσεις της γωνίας των $80°$ θα προέκυπτε ότι η γωνία των $20°$ είναι κατασκευάσιμη, το οποίο αντιβαίνει στο **Λήμμα 2.4**.

Έστω θ μια γωνία και σημεία X, O, Y τέτοια ώστε $\widehat{XOY} = \theta$. Από το O φέρουμε κύκλο C ακτίνας 1 και θεωρούμε τα σημεία τομής $A = C \cap \underrightarrow{OY}$ και $B = C \cap \underrightarrow{OX}$. Έπειτα, φέρουμε τη μεσοκάθετη μ του AB και παρατηρούμε ότι:

$$\widehat{AO[\mu \cap AB]} = \frac{1}{2}\widehat{AOB} = \frac{\theta}{2}$$

το οποίο είναι το ζητούμενο.

$\square$

Άσκηση 3 Εξετάστε ποιές από τις ακόλουθες επεκτάσεις K είναι σώματα ριζών πάνω από το F.

i. $K = \mathbb{Q}(i)$, $F = \mathbb{Q}$,

ii. $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$, $F = \mathbb{Q}$,

iii. $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$, $F = \mathbb{Q}(\sqrt[3]{3})$,

iv. $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, i)$, $F = \mathbb{Q}$.

Λήμμα 3.1: *Το* $\sqrt{3}$ *δεν ανήκει στο* $\mathbb{Q}(\sqrt[3]{3})$.

Απόδειξη: Πράγματι, σε διαφορετική περίπτωση θα αληθεύει ο εγκλεισμός των σωμάτων $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt[3]{3})$. Αυτό αντιβαίνει στο *Θεώρημα των Πύργων*, αφού η επέκταση $\mathbb{Q}(\sqrt{3})$ έχει βαθμό 2 και η $\mathbb{Q}(\sqrt[3]{3})$ έχει βαθμό 3 υπεράνω του $\mathbb{Q}$.

$\triangle$

$\boxed{\text{i.}}$ *Λύση:* Το πολυώνυμο $x^2 + 1 \in \mathbb{Q}[x]$ είναι ανάγωγο στο $\mathbb{Q}$ αφού είναι ανάγωγο στο υπέρσωμα $\mathbb{R}$. Επιπλέον, οι ρίζες του $x^2 + 1$ είναι οι $\pm i$, οι οποίες αμφότερες ανήκουν στο $\mathbb{Q}(i)$. Κατ' επέκταση, το $x^2 + 1$ αναλύεται πλήρως στο $\mathbb{Q}(i)$:

$$x^2 + 1 = (x + i)(x - i)$$

το οποίο δείχνει ότι το $\mathbb{Q}(i)$ είναι σώμα ριζών του $x^2 + 1$ πάνω από το $\mathbb{Q}$.

$\square$

$\boxed{\text{ii.}}$ *Λύση:* Υποθέτουμε προς άτοπο ότι η επέκταση $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$ του $\mathbb{Q}$ είναι σώμα ριζών κάποιου πολυωνύμου, οπότε και η επέκταση K του $\mathbb{Q}(\sqrt{3})$ είναι σώμα ριζών κάποιου πολυωνύμου.

$$\begin{tikzcd} K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) \arrow[d, dash] \\ \mathbb{Q}(\sqrt{3}) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Η τελευταία, ως πεπερασμένη επέκταση και σώμα ριζών, αποτελεί κανονική επέκταση - οπότε κάθε ανάγωγο πολυώνυμο του $\mathbb{Q}(\sqrt{3})[x]$ αναλύεται πλήρως στο K. Ειδικότερα, θα δείξουμε ότι το $x^3 - 3$ είναι ανάγωγο στο $\mathbb{Q}(\sqrt{3})[x]$, οπότε οι ρίζες του ανήκουν όλες στο K.

Για την απόδειξη του ισχυρισμού, επειδή ο βαθμός του πολυωνύμου είναι $2 \leqslant 3$, αρκεί να αποδειχθεί ότι οι ρίζες του $x^3 - 3$ δεν ανήκουν στο $\mathbb{Q}(\sqrt{3})$. Πράγματι, επειδή οι ρίζες του είναι η $\sqrt[3]{3}$ και δύο συζυγείς μιγαδικές, σε συνδυασμό με το **Λήμμα 3.1** αποδεικνύεται ότι το $x^3 - 3$ δεν έχει ρίζες στο $\mathbb{Q}(\sqrt{3})$.

Συμβολίζουμε με $\omega, \bar{\omega}$ τις δύο συζυγείς μιγαδικές ρίζες τρίτης τάξεως της μονάδος (δηλ. $\omega^2 + \omega + 1 = 0$), και παρατηρούμε ότι οι ρίζες του $x^3 - 3$ είναι ακριβώς οι $\sqrt[3]{3}, \omega\sqrt[3]{3}, \bar{\omega}\sqrt[3]{3}$. Υπο τις υποθέσεις μας λοιπόν, συγκεκριμένα οι δύο μιδαγικές θα πρέπει να ανήκουν στο σώμα $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$, το οποίο φυσικά είναι άτοπο, αφού το εν λόγω σώμα είναι υποσύνολο των πραγματικών.

□

$\boxed{\text{iii.}}$ *Λύση:* Κατ' αρχήν παρατηρούμε ότι το πολυώνυμο $x^2 - 3$ μπορεί να θεωρηθεί στο $\mathbb{Q}(\sqrt[3]{3})$. Επειδή αυτό έχει ρίζες τις $\pm\sqrt{3}$, το αντίστοιχο σώμα ριζών του θα είναι το $\mathbb{Q}(-\sqrt{3}, \sqrt{3}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$, δηλαδή θα είναι το K.

□

$\boxed{\text{iv.}}$ *Λύση:* Στο υποερώτημα ii. δείξαμε ότι το πολυώνυμο $x^3 - 3$ αναλύεται πλήρως στο $\mathbb{C}$ ως εξής:

$$x^3 - 3 = (x - \sqrt[3]{3})(x - \omega\sqrt[3]{3})(x - \bar{\omega}\sqrt[3]{3})$$

Επιπλέον, η ανάλυση του $x^2 - 3$ στο $\mathbb{C}$ είναι η $(x - \sqrt{3})(x + \sqrt{3})$, επομένως το πολυώνυμο:

$$P(x) = (x^2 - 3)(x^3 - 3) = (x - \sqrt{3})(x + \sqrt{3})(x - \sqrt[3]{3})(x - \omega\sqrt[3]{3})(x - \bar{\omega}\sqrt[3]{3})$$

έχει σώμα ριζών το $\mathbb{Q}(-\sqrt{3}, \sqrt{3}, \sqrt[3]{3}, \omega\sqrt{3}, \bar{\omega}\sqrt{3}) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \omega)$. Επειδή τώρα μπορούμε να θεωρήσουμε:

$$\omega = \frac{1 + i\sqrt{3}}{2} \text{ (ίσο δηλαδή με την πρώτη κατά την αριστερόστροφη φορά ρίζα)}$$

έπεται ότι το ω ανήκει στο $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, i)$. Κατ' επέκταση, $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \omega) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, i)$. Ο αντίστροφος εγκλεισμός '$\supseteq$' ισχύει κι αυτός, αφού η μορφή:

$$\frac{\omega - \bar{\omega}}{2\sqrt{3}} = \frac{2i\sqrt{3}}{2\sqrt{3}} = i$$

ανήκει στο $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \omega)$. Ισχύει λοιπόν η ισότητα συνόλων $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, i) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, \omega)$, οπότε η επέκταση $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}, i)$ του $\mathbb{Q}$ αποτελεί σώμα ριζών του P.

□

Άσκηση 4 Έστω $f(x) = x^3 - a \in \mathbb{Q}[x]$ και $K \subseteq \mathbb{C}$ το σώμα των ριζών του $f(x)$ στο $\mathbb{C}$. Για κάθε $n \in [7]$, δώστε παράδειγμα ενός a τέτοιο ώστε $[K : \mathbb{Q}] = n$, εάν φυσικά τέτοιο a υπάρχει. Διαφορετικά, αποδείξτε ότι a με αυτήν την ιδιότητα δεν υπάρχει. ■

Λύση: Ας συμβολίσουμε με $\omega, \bar{\omega}$ τις δύο μιγαδικές τρίτες ρίζες της μονάδος. Το πολυώνυμο $x^3 - a \in \mathbb{Q}[x]$ αναλύεται πλήρως στο $\mathbb{C}$ και παίρνει τη μορφή:

$$x^3 - a = (x - \sqrt[3]{a})(x - \omega\sqrt[3]{a})(x - \bar{\omega}\sqrt[3]{3})$$

Επομένως, το σώμα ριζών του θα έχει τη μορφή $K = \mathbb{Q}(\sqrt[3]{a}, \omega\sqrt[3]{a}, \bar{\omega}\sqrt[3]{a})$.

$$\begin{tikzcd}
K = \mathbb{Q}(\sqrt[3]{a}, \bar{\omega}\sqrt[3]{a}) \arrow[rr, equal] \arrow[dr, dash] & & \mathbb{Q}(\sqrt[3]{a}, \omega\sqrt[3]{a}) \arrow[dl, dash] \\
& \mathbb{Q}(\sqrt[3]{a}) \arrow[d, dash] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Παρατηρούμε ότι ο βαθμός $\ell = [K : \mathbb{Q}(\sqrt[3]{a})]$ είναι ακριβώς 2, αφού είναι το πολύ 2 (το πολυώνυμο $x^2 + \sqrt[3]{a}x + (\sqrt[3]{a})^2$ μηδενίζεται από τα $\omega\sqrt[3]{a}$ και $\bar{\omega}\sqrt[3]{a}$) και τα σώματα $K, \mathbb{Q}(\sqrt[3]{a})$ δεν ταυτίζονται. Επιπλέον, ο βαθμός $\delta = [\mathbb{Q}(\sqrt[3]{a}) : \mathbb{Q}]$ είναι το πολύ 3, αφού το πολυώνυμο $x^3 - a$ μηδενίζεται από το $\sqrt[3]{a}$. Έχουμε λοιπόν το ακόλουθο πόρισμα:

Πόρισμα: *Εάν υπάρχει f τέτοιο ώστε η επέκταση K του $\mathbb{Q}$ να αποτελεί σώμα ριζών του f, τότε αυτή έχει άρτιο βαθμό, το πολύ 6.*

△

Δεδομένου του πορίσματος, ακρεί να διερευνηθούν οι περιπτώσεις $n \in \{2, 4, 6\}$.

Περίπτωση $\mathbf{n = 2}$: Θεωρούμε οποινδήποτε ρητό $a \in \mathbb{Q}_3 := \{p^3 \mid p \in \mathbb{Q}\}$ και παρατηρούμε ότι η επέκταση $[Q(\sqrt[3]{a}) : \mathbb{Q}]$ έχει βαθμό $\delta = 1$. Κατ' επέκταση, $n = 2$, αφού $\ell = 2$.

Περίπτωση $\mathbf{n = 4}$ και $\mathbf{n = 6}$: Από την προηγούμενη περίπτωση έπεται ότι $a \notin \mathbb{Q}_3$. Εάν $a \notin \mathbb{Q}_3$ και $a \in \mathbb{Q}$, τότε το πολυώνυμο $x^3 - a$ δεν έχει ρίζες στο $\mathbb{Q}$ οπότε είναι ανάγωγο. Κατ' επέκταση, ο βαθμός n, εάν δεν είναι 2, είναι $n = \ell \cdot \delta = 2 \cdot 3 = 6$.

□