ΤΟ «ΠΡΑΓΜΑΤΙΚΟ» ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΤΗΣ ΑΛΓΕΒΡΑΣ

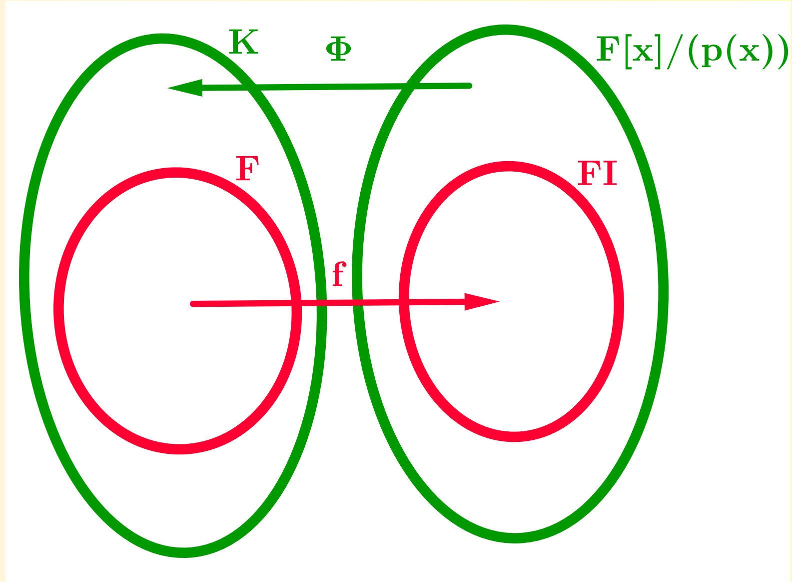
Γνωρίζουμε ως Θεμελιώδες Θεώρημα της Άλγεβρας την πρόταση,

Κάθε πολυώνυμο βαθμού n με συντελεστές στο $\mathbb{C}$ έχει ακριβώς n το πλήθος ρίζες στο $\mathbb{C}$, (λαμβάνοντας υπ΄ όψιν το πλήθος των εμφανίσεων της κάθε ρίζας).

ΤΟ «ΠΡΑΓΜΑΤΙΚΟ» ΘΕΜΕΛΙΩΔΕΣ ΘΕΩΡΗΜΑ ΤΗΣ ΑΛΓΕΒΡΑΣ
Ή ΘΕΩΡΗΜΑ GIRARD–KRONECKER

Για κάθε πολυώνυμο βαθμού n με συντελεστές σε κάποιο σώμα F υπάρχει σώμα L ώστε $\mathbf{F} \subseteq \mathbf{L}$ και το L περιέχει ακριβώς n το πλήθος ρίζες του πολυωνύμου, (λαμβάνοντας υπ΄ όψιν το πλήθος των εμφανίσεων της κάθε ρίζας).

- Ο Albert Girard (1595–1632) το 1629 διατύπωσε γραπτώς, (Invention Nouvelle en l'Algebre), και χωρίς απόδειξη πρόταση με Μαθηματικό νόημα παραπλήσιο της πρότασης που σήμερα ονομάζουμε Θεμελιώδες Θεώρημα της Άλγεβρας.
- Για πολλά χρόνια η αλήθεια της πρότασης θεωρείτο και λαμβάνετο ως δεδομένη και δεν υπήρξε προσπάθεια απόδειξής της.
- Διαδοχικές προσπάθειες απόδειξης από τους d'Alambert (1717–1783), Euler (1707–1783), Foncenex (1734–1799), Lagrange (1736–1813), Gauss (1777-1855). Το Θεμελιώδες Θεώρημα της Άλγεβρας είναι υποπερίπτωση του γενικότερου θεωρήματος GIRARD–KRONECKER. Το Θεμελιώδες Θεώρημα της Άλγεβρας ουσιαστικώς λέει ότι αν $F = \mathbb{C}$ τότε και $L = \mathbb{C}$.
- Το θεώρημα GIRARD–KRONECKER απέδειξε ο KRONECKER στηριζόμενος στην πιο κάτω κατασκευαστική ιδέα, (με $p(x)$ ανάγωγο πολυώνυμο),



Από το δοθέν σώμα F των συντελεστών του πολυωνύμου, και μέσω κατάλληλου ισομορφισμού f, κατασκευάζεται το σώμα FI με ίδιες ακριβώς αλγεβρικές ιδιότητες με αυτές του F. Αποδεικνύεται ότι το $F[x]/(p(x))$ είναι υπερσώμα του FI που περιέχει μία ρίζα της ισομορφικής εικόνας του δοθέντος πολυωνύμου.

Στην βιβλιογραφία, η κατασκευή του $\mathbf{K} \supseteq \mathbf{F}$ που περιέχει μία ρίζα του δοθέντος πολυωνύμου παραλείπεται. Αφήνεται ως άσκηση στον αναγνώστη. Σκοπός μας είναι, παρουσιάζοντας την διαδικασία κατασκευής του σώματος $\mathbf{F[x]/(p(x))}$, να παρουσιάσουμε και την κατασκευή του σώματος $\mathbf{K}$ που περιέχει μία ρίζα του δοθέντος πολυωνύμου και κατ΄ επέκταση του σώματος $\mathbf{L}$ που περιέχει όλες τις ρίζες του.

- Κάθε σύνολο F εφοδιασμένο με δύο πράξεις τέτοιες ώστε η πρώτη από αυτές να έχει ίδιες αλγεβρικές ιδιότητες με την πρόσθεση του $\mathbb{Z}$ και η δεύτερη να έχει ίδιες αλγεβρικές ιδιότητες με τον πολλαπλασιασμό του $\mathbb{Z}$ λέγεται μεταθετικός δακτύλιος με μονάδα.
- Αν επιπλέον η δεύτερη πράξη έχει ίδιες αλγεβρικές ιδιότητες με τον πολλαπλασιασμό του $\mathbb{Q}$ τότε το σύνολο λέγεται σώμα.
- Οι πράξεις αυτές αναφέρονται ως «πρόσθεση» και «πολλαπλασιασμός» ακόμα κι όταν δεν είναι η συνήθης πρόσθεση και ο συνήθης πολλαπλασιασμός των $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ που γνωρίζουμε. Συμβολίζουμε τις πράξεις αυτές είτε ως «$+$», «$\cdot$» είτε ως «$\oplus$», «$\odot$» και τον πολλαπλασιασμό κάποιες φορές με κενό.
- Όταν το F είναι σώμα, το σύνολο $F[x] = \{\Sigma_{i=0}^{n} a_i\, x^i \,:\, a_i \in\ F,\, n \in \mathbb{N}\}$ είναι ο δακτύλιος των πολυωνύμων με συντελεστές στο σώμα F. Η πρόσθεση και ο πολλαπλασιασμός στο $F[x]$ ορίζονται κατ΄ αναλογία των αντιστοίχων πράξεων στο $\mathbb{Q}[x]$ δηλαδή, $\forall\, f(x) = \Sigma_{i=0}^{n} a_i\, x^i, g(x) = \Sigma_{i=0}^{m} \beta_i\, x^i \in F[x]$,
  $f(x) + g(x) = \Sigma_{i=0}^{max\{n,m\}} (a_i + \beta_i)\, x^i$, $f(x)\, g(x) = \Sigma_{i=0}^{n+m} \left[\Sigma_{j=0}^{i} a_{i-j}\, \beta_j\right] x^i$.

- Έστω F σώμα, $p(x) \in F[x]$, $deg[p(x)] \geq 1$. Λέμε ότι το $p(x)$ είναι ανάγωγο στο $F[x]$ αν δεν υπάρχουν $a(x), b(x) \in F[x]$ ώστε $deg[a(x)] \geq 1$, $deg[b(x)] \geq 1$ και $p(x) = a(x)\, b(x)$.

Έστω $\mathbf{b(x), p(x) \in F[x]}$. Ορίζουμε το σύνολο $\mathbf{b(x) + (p(x))}$ ως εξής,

$$\mathbf{b(x) + (p(x)) = \{b(x) + a(x)\, p(x) : a(x) \in F[x]\}.}$$

Ορίζουμε το σύνολο $\mathbf{F[x]/(p(x))}$ ως εξής,

$$\mathbf{F[x]/(p(x)) = \{b(x) + (p(x)) : b(x) \in F[x]\}.}$$

Στην βιβλιογραφία χρησιμοποιούνται εκτεταμένως οι δύο συμβολισμοί $\mathbf{F[x]/(p(x))}$ και $\mathbf{F[x]/\langle p(x)\rangle}$ με το ίδιο νόημα. Στα επόμενα θα χρησιμοποιήσουμε τον συμβολισμό $\mathbf{F[x]/\langle p(x)\rangle}$ για να αποφύγουμε τις πολλές παρενθέσεις. Άρα,

$$\begin{aligned}\mathbf{b(x) + \langle p(x)\rangle} &= \mathbf{\{b(x) + a(x)\, p(x) : a(x) \in F[x]\},}\\ \mathbf{F[x]/\langle p(x)\rangle} &= \mathbf{\{b(x) + \langle p(x)\rangle : b(x) \in F[x]\}.}\end{aligned}$$

Εφοδιάζουμε το $F[x]/\langle p(x)\rangle$ με μία πράξη πρόσθεσης $\oplus$ και μία πράξη πολλαπλασιασμού $\odot$ ως εξής,

$$\begin{aligned}(b_1(x)+\langle p(x)\rangle)\oplus(b_2(x)+\langle p(x)\rangle) &= (b_1(x)+b_2(x))+\langle p(x)\rangle,\\ (b_1(x)+\langle p(x)\rangle)\odot(b_2(x)+\langle p(x)\rangle) &= (b_1(x)\,b_2(x))+\langle p(x)\rangle.\end{aligned}$$

- Το $F[x]/\langle p(x)\rangle$ είναι κλειστό ως προς τις πράξεις $\oplus, \odot$.
- Επειδή, $(b_1(x)+\langle p(x)\rangle)\oplus(b_2(x)+\langle p(x)\rangle) =$

$$\begin{aligned}&= (b_1(x)+b_2(x))+\langle p(x)\rangle =\\ &= (b_2(x)+b_1(x))+\langle p(x)\rangle =\\ &= (b_2(x)+\langle p(x)\rangle)\oplus(b_1(x)+\langle p(x)\rangle),\end{aligned}$$

και $(b_1(x)+\langle p(x)\rangle)\odot(b_2(x)+\langle p(x)\rangle) = (b_1(x)\,b_2(x))+\langle p(x)\rangle =$

$$\begin{aligned}&= (b_2(x)\,b_1(x))+\langle p(x)\rangle =\\ &= (b_2(x)+\langle p(x)\rangle)\odot(b_1(x)+\langle p(x)\rangle),\end{aligned}$$

οι πράξεις $\oplus, \odot$ είναι μεταθετικές.

- Τα $0+\langle p(x)\rangle=\langle p(x)\rangle$, $1+\langle p(x)\rangle$ είναι τα ουδέτερα στοιχεία των πράξεων $\oplus, \odot$ αντιστοίχως.
- Το $-b(x)+\langle p(x)\rangle$ είναι το αντίθετο του $b(x)+\langle p(x)\rangle$ όταν $b(x)\neq 0$.
- Επειδή, $((b_1(x)+\langle p(x)\rangle)\oplus(b_2(x)+\langle p(x)\rangle))\oplus(b_3(x)+\langle p(x)\rangle)=$

$$\begin{aligned}
&= ((b_1(x)+b_2(x))+\langle p(x)\rangle)\oplus(b_3(x)+\langle p(x)\rangle)=\\
&= ((b_1(x)+b_2(x))+b_3(x))+\langle p(x)\rangle=\\
&= (b_1(x)+(b_2(x)+b_3(x)))+\langle p(x)\rangle=\\
&= (b_1(x)+\langle p(x)\rangle)\oplus((b_2(x)+b_3(x))+\langle p(x)\rangle)=\\
&= (b_1(x)+\langle p(x)\rangle)\oplus((b_2(x)+\langle p(x)\rangle)\oplus(b_3(x)+\langle p(x)\rangle)),
\end{aligned}$$

και $((b_1(x)+\langle p(x)\rangle)\odot(b_2(x)+\langle p(x)\rangle))\odot(b_3(x)+\langle p(x)\rangle)=$

$$\begin{aligned}
&= ((b_1(x)\,b_2(x))+\langle p(x)\rangle)\odot(b_3(x)+\langle p(x)\rangle)=\\
&= ((b_1(x)\,b_2(x))\,b_3(x))+\langle p(x)\rangle=\\
&= (b_1(x)\,(b_2(x)\,b_3(x)))+\langle p(x)\rangle=\\
&= (b_1(x)+\langle p(x)\rangle)\odot((b_2(x)\,b_3(x))+\langle p(x)\rangle)=\\
&= (b_1(x)+\langle p(x)\rangle)\odot((b_2(x)+\langle p(x)\rangle)\odot(b_3(x)+\langle p(x)\rangle)),
\end{aligned}$$

οι πράξεις $\oplus, \odot$ είναι προσεταιριστικές.

- Επειδή, $((b_1(x)+\langle p(x)\rangle)\odot((b_2(x)+\langle p(x)\rangle)\oplus(b_3(x)+\langle p(x)\rangle)) =$

$$\begin{aligned}
&= (b_1(x)+\langle p(x)\rangle)\odot((b_2(x)+b_3(x))+\langle p(x)\rangle) = \\
&= (b_1(x)\,(b_2(x)+b_3(x))+\langle p(x)\rangle = \\
&= (b_1(x)\,b_2(x)+b_1(x)\,b_3(x))+\langle p(x)\rangle = \\
&= (b_1(x)\,b_2(x)+\langle p(x)\rangle)\oplus(b_1(x)\,b_3(x)+\langle p(x)\rangle) = \\
&= (b_1(x)+\langle p(x)\rangle)\odot(b_2(x)+\langle p(x)\rangle)\oplus \\
&\quad \oplus(b_1(x)+\langle p(x)\rangle)\odot(b_3(x)+\langle p(x)\rangle),
\end{aligned}$$

ισχύει η επιμεριστική ιδιότητα του «πολλαπλασιασμού» $\odot$ επί της «πρόσθεσης» $\oplus$. Το $F[x]/\langle p(x)\rangle$ εφοδιασμένο με την «πρόσθεσης» $\oplus$ και τον «πολλαπλασιασμό» $\odot$ είναι μεταθετικός δακτύλιος με μονάδα.

Έστω $\mathbf{p}(\mathbf{x})$ ένα ανάγωγο πολυώνυμο του $\mathbf{F}[\mathbf{x}]$. Το σύνολο $\mathbf{F}[\mathbf{x}]/\langle\mathbf{p}(\mathbf{x})\rangle$ εφοδιασμένο με τις πράξεις $\oplus,\odot$ είναι σώμα.

Αρκεί να δείξουμε ότι για κάθε μη μηδενικό στοιχείο του $F[x]/\langle p(x)\rangle$ υπάρχει «πολλαπλασιαστικό» αντίστροφο ως προς τον «πολλαπλασιασμό» $\odot$. Έστω $b(x)+\langle p(x)\rangle$ μη μηδενικό στοιχείο του $F[x]/\langle p(x)\rangle$ δηλαδή, $b(x)+\langle p(x)\rangle\neq 0+\langle p(x)\rangle=\langle p(x)\rangle$. Άρα, $b(x)+\langle p(x)\rangle\neq\langle p(x)\rangle$. Αν το $p(x)$ διαιρεί το $b(x)$ τότε, $b(x)=p(x)\,q(x)$, με $q(x)\in F[x]$ δηλαδή, $b(x)\in\langle p(x)\rangle$ και

$$\begin{aligned} b(x)+\langle p(x)\rangle &= \{b(x)+a(x)\,p(x) : a(x)\in F[x]\} = \\ &= \{p(x)\,q(x)+a(x)\,p(x) : q(x), a(x)\in F[x]\} = \\ &= \{(q(x)+a(x))\,p(x) : q(x), a(x)\in F[x]\} = \\ &= \{g(x)\,p(x) : g(x)\in F[x]\} = \langle p(x)\rangle, \end{aligned}$$

άτοπο. Άρα το $p(x)$ δεν διαιρεί το $b(x)$. Έστω $d(x)\in F[x]$ είναι ένας μέγιστος κοινός διαιρέτης των $p(x)$, $b(x)$. Αν $deg[d(x)]\geq 1$ τότε η σχέση $p(x)=d(x)\,k(x)$, με $k(x)\in F[x]$ επάγει ότι $deg[k(x)]=0$, (γιατί το $p(x)$ είναι ανάγωγο). Οπότε, $k(x)=k\in F-\{0\}$ και $p(x)=k\,d(x)$ ή $d(x)=k^{-1}\,p(x)$. Από την $b(x)=d(x)\,t(x)$ με $t(x)\in F[x]$ έπεται $b(x)=k^{-1}\,t(x)\,p(x)$ και το $p(x)$ διαιρεί το $b(x)$, άτοπο.

Άρα, τα $p(x)$, $b(x)$ είναι πρώτα μεταξύ τους και από γνωστή ιδιότητα των σχετικώς πρώτων πολυωνύμων μπορούμε να γράψουμε,

$$\begin{aligned} b_1(x)\,b(x)+b_2(x)\,p(x)=1 \Rightarrow (\text{ με } b_1(x),\ b_2(x)\in F[x]) & \\ b_1(x)\,b(x)=1+(-b_2(x))\,p(x) & \ \Rightarrow \\ (b_1(x)+\langle p(x)\rangle)\odot(b(x)+\langle p(x)\rangle)=(b_1(x)\,b(x))+\langle p(x)\rangle & \ = \\ \{b_1(x)\,b(x)+a(x)\,p(x) : a(x)\in F[x]\} & \ = \end{aligned}$$

$$\begin{aligned}\{1+(-b_2(x))\,p(x)+a(x)\,p(x) : -b_2(x), a(x)\in F[x]\} &= \\ \{1+(-b_2(x)+a(x))\,p(x) : -b_2(x), a(x)\in F[x]\} &= \\ \{1+u(x)\,p(x) : u(x)\in F[x]\} &= \\ 1+\langle p(x)\rangle.\end{aligned}$$

Δείξαμε ότι το μη μηδενικό στοιχείο $b(x)+\langle p(x)\rangle$ του $F[x]/\langle p(x)\rangle$ έχει αντίστροφο ως προς την πράξη $\odot$ και το $F[x]/\langle p(x)\rangle$ είναι σώμα.

Θεωρούμε το σύνολο $\mathbf{FI} = \{\mathbf{b}+\langle \mathbf{p}(\mathbf{x})\rangle : \mathbf{b}\in \mathbf{F}\}$, $\mathbf{p}(\mathbf{x})$ ανάγωγο πολυώνυμο του $\mathbf{F}[\mathbf{x}]$. Το $\mathbf{FI}$ είναι υποσύνολο του $\mathbf{F}[\mathbf{x}]/\langle \mathbf{p}(\mathbf{x})\rangle$. Ορίζουμε την συνάρτηση $\mathbf{f} : \mathbf{F}\mapsto \mathbf{FI}$ με κανόνα $\mathbf{f}(\mathbf{b}) = \mathbf{b}+\langle \mathbf{p}(\mathbf{x})\rangle$. Η συνάρτηση αυτή είναι ισομορφική εμφύτευση του σώματος $\mathbf{F}$ στο σώμα $\mathbf{F}[\mathbf{x}]/\langle \mathbf{p}(\mathbf{x})\rangle$.

Έστω $b_1 = b_2$ στοιχεία του F. Τότε και $b_1 - b_2 = 0$ και,

$$\begin{aligned}(b_1-b_2)+\langle p(x)\rangle &= \{(b_1-b_2)+a(x)\,p(x) : a(x)\in F[x]\} = \\ &= \{0+a(x)\,p(x) : a(x)\in F[x]\} = \\ &= \{a(x)\,p(x) : a(x)\in F[x]\} =\end{aligned}$$

$$\begin{aligned} &= \langle p(x)\rangle = 0 + \langle p(x)\rangle \Rightarrow \\ (b_1 + \langle p(x)\rangle) - (b_2 + \langle p(x)\rangle) &= 0 + \langle p(x)\rangle \Rightarrow \\ b_1 + \langle p(x)\rangle &= b_2 + \langle p(x)\rangle, \end{aligned}$$

και η f είναι καλώς ορισμένη. Επίσης,

$$\begin{aligned} b_1 + \langle p(x)\rangle &= b_2 + \langle p(x)\rangle \Rightarrow \\ (b_1 - b_2) + \langle p(x)\rangle &= 0 + \langle p(x)\rangle = \langle p(x)\rangle \Rightarrow \\ \{(b_1 - b_2) + a(x)\,p(x) : a(x) \in F[x]\} &= \{a(x)\,p(x) : a(x) \in F[x]\} \Rightarrow \\ (b_1 - b_2) + a_1(x)\,p(x) &= a_2(x)\,p(x) \Rightarrow \\ &\quad \text{για κάποια } a_1(x),\ a_2(x) \in F[x] \\ b_1 - b_2 &= (a_1(x) - a_2(x))\,p(x). \end{aligned}$$

Αν $a_1(x) \neq a_2(x)$ τότε το $p(x)$ βαθμού μεγαλύτερου ή ίσου του 1, (ως ανάγωγο), διαιρεί το σταθερό πολυώνυμο $b_1 - b_2$. Αυτό μπορεί να συμβαίνει μόνο αν το $b_1 - b_2$ είναι το μηδενικό πολυώνυμο δηλαδή, $b_1 = b_2$. Αν $a_1(x) = a_2(x)$ τότε $b_1 - b_2 = 0\,p(x) = 0$ και $b_1 = b_2$. Αποδείξαμε ότι η f είναι ένα προς ένα.

$$\begin{aligned} f(b_1+b_2) &= (b_1+b_2)+\langle p(x)\rangle = (b_1+\langle p(x)\rangle)\oplus(b_2+\langle p(x)\rangle) = \\ &= f(b_1)\oplus f(b_2), \\ f(b_1\,b_2) &= (b_1\,b_2)+\langle p(x)\rangle = (b_1+\langle p(x)\rangle)\odot(b_2+\langle p(x)\rangle) = \\ &= f(b_1)\odot f(b_2). \end{aligned}$$

Η f απεικονίζει τις πράξεις του σώματος F στις πράξεις του σώματος $F[x]/\langle p(x)\rangle$ όταν αυτές σημειώνονται ανάμεσα στα σταθερά στοιχεία του $F[x]/\langle p(x)\rangle$. Τα σταθερά στοιχεία του $F[x]/\langle p(x)\rangle$ συγκροτούν το σύνολο FI. Για κάθε $b+\langle p(x)\rangle \in FI$ υπάρχει στοιχείο του F το b ώστε $f(b)=b+\langle p(x)\rangle$ επάγοντας ότι η f είναι επί του FI.

Τελικώς έχουμε δείξει ότι η συνάρτηση f είναι ένας ένα προς ένα και επί ομομορφισμός από το σώμα F στο σύνολο FI. Δηλαδή η f είναι ένα ισομορφισμός από το σώμα F στο σύνολο FI και άρα επάγει στο FI δομή σώματος με τις πράξεις $\oplus, \odot$.

Το σύνολο $\mathbf{FI[x]} = \{\Sigma_{k=0}^{n}(b_k + \langle p(x)\rangle)\, x^k : n \in \mathbb{N},\ b_k \in F\}$ εφοδιασμένο με τις πράξεις «πρόσθεσης» $\oplus$ και «πολλαπλασιασμού» $\odot$ ώστε,

$$\Sigma_{k=0}^{n}(b_k + \langle p(x)\rangle)\, x^k \oplus \sum_{k=0}^{m}(g_k + \langle p(x)\rangle)\, x^k = \Sigma_{k=0}^{\max\{n,m\}}((b_k + \langle p(x)\rangle) \oplus (g_k + \langle p(x)\rangle))\, x^k,$$

$$\Sigma_{k=0}^{n}(b_k + \langle p(x)\rangle)\, x^k \odot \sum_{k=0}^{m}(g_k + \langle p(x)\rangle)\, x^k = \Sigma_{k=0}^{n+m}\left(\sum_{i=0}^{k}(b_{k-i} + \langle p(x)\rangle) \odot (g_i + \langle p(x)\rangle)\right) x^k,$$

είναι δακτύλιος πολυωνύμων.

Είναι άμεση εφαρμογή των ιδιοτήτων των πράξεων του F και του FI να δείξουμε ότι το $FI[x]$ είναι δακτύλιος.

Έστω οι δακτύλιοι πολυωνύμων $\mathbf{F[x]}$, $\mathbf{FI[x]}$. Μέσω της συνάρτησης $\mathbf{f : F \mapsto FI}$ ορίζουμε την συνάρτηση,

$$\mathcal{F} : \mathbf{F[x]} \mapsto \mathbf{FI[x]}$$

με κανόνα,

$$\mathcal{F}(\mathbf{b}(\mathbf{x})) = \mathcal{F}\left(\boldsymbol{\Sigma}_{\mathbf{k=0}}^{\mathbf{n}}\mathbf{b_k}\,\mathbf{x^k}\right) = \boldsymbol{\Sigma}_{\mathbf{k=0}}^{\mathbf{n}}\mathbf{f}(\mathbf{b_k})\,\mathbf{x^k}.$$

Η $\mathcal{F}$ είναι ισομορφισμός δακτυλίων πολυωνύμων.

Αν $b(x) = \Sigma_{k=0}^{n} b_k\, x^k = \Sigma_{k=0}^{m} g_k\, x^k = g(x)$ τότε $n = m$, $b_k = g_k$ και $f(b_k) = f(g_k)$ γιατί η f είναι καλώς ορισμένη. Οπότε,

$$\mathcal{F}(b(x)) = \sum_{k=0}^{n} f(b_k)\, x^k = \sum_{k=0}^{m} f(g_k)\, x^k = \mathcal{F}(g(x)),$$

και η $\mathcal{F}$ είναι καλώς ορισμένη. Ενώ,

$$\mathcal{F}(b(x)) = \mathcal{F}\left(\Sigma_{k=0}^{n} b_k\, x^k\right) = \mathcal{F}\left(\Sigma_{k=0}^{m} g_k\, x^k\right) = \mathcal{F}(g(x)) \Rightarrow$$

$$\Sigma_{k=0}^{n} f(b_k)\, x^k = \Sigma_{k=0}^{m} f(g_k)\, x^k,$$

και $n = m$, $f(b_k) = f(g_k)$ που επάγει $b_k = g_k$ επειδή η f είναι ένα προς ένα. Άρα,

$$b(x) = \Sigma_{k=0}^{n} b_k\, x^k = \Sigma_{k=0}^{m} g_k\, x^k = g(x),$$

και η $\mathcal{F}$ είναι ένα προς ένα. Για κάθε πολυώνυμο,

$$B(x) = \Sigma_{k=0}^{n}(b_k + \langle p(x)\rangle)\, x^k = \Sigma_{k=0}^{n} f(b_k)\, x^k,$$

του $FI[x]$, υπάρχει το πολυώνυμο $b(x) = \Sigma_{k=0}^{n} b_k\, x^k$ του $F[x]$ ώστε $\mathcal{F}(b(x)) = B(x)$ και η $\mathcal{F}$ είναι επί του FI.

$$
\begin{aligned}
\mathcal{F}(b(x)+g(x)) &= \mathcal{F}\left(\Sigma_{k=0}^{\max\{n,m\}}(b_k+g_k)\,x^k\right) = \Sigma_{k=0}^{\max\{n,m\}} f(b_k+g_k)\,x^k = \\
&= \Sigma_{k=0}^{\max\{n,m\}}((b_k+g_k)+\langle p(x)\rangle)\,x^k = \\
&= \Sigma_{k=0}^{\max\{n,m\}}((b_k+\langle p(x)\rangle)\oplus(g_k+\langle p(x)\rangle))\,x^k = \\
&= \Sigma_{k=0}^{n}(b_k+\langle p(x)\rangle)\,x^k \oplus \Sigma_{k=0}^{m}(g_k+\langle p(x)\rangle)\,x^k = \\
&= \Sigma_{k=0}^{n} f(b_k)\,x^k \oplus \Sigma_{k=0}^{m} f(g_k)\,x^k = \\
&= \mathcal{F}(b(x))\oplus\mathcal{F}(g(x)), \\
\mathcal{F}(b(x)\,g(x)) &= \mathcal{F}\left(\Sigma_{k=0}^{n} b_k\,x^k\,\Sigma_{k=0}^{m} g_k\,x^k\right) = \mathcal{F}\left(\Sigma_{k=0}^{n+m}\left(\Sigma_{i=0}^{k} b_{k-i}\,g_i\right)x^k\right) = \\
&= \Sigma_{k=0}^{n+m}\left(\Sigma_{i=0}^{k} f(b_{k-i}\,g_i)\right)x^k = \\
&= \Sigma_{k=0}^{n+m}\left(\Sigma_{i=0}^{k}(b_{k-i}+\langle p(x)\rangle)\odot(g_i+\langle p(x)\rangle)\right)x^k = \\
&= \Sigma_{k=0}^{n}(b_k+\langle p(x)\rangle)\,x^k \odot \Sigma_{k=0}^{m}(g_k+\langle p(x)\rangle)\,x^k = \\
&= \Sigma_{k=0}^{n} f(b_k)\,x^k \odot \Sigma_{k=0}^{m} f(g_k)\,x^k = \\
&= \mathcal{F}(b(x))\odot\mathcal{F}(g(x)),
\end{aligned}
$$

και η $\mathcal{F}$ είναι ομομορφισμός δακτυλίων πολυωνύμων. Άρα η $\mathcal{F}$ είναι ένα προς ένα, επί και ομομορφισμός δηλαδή ισομορφισμός δακτυλίων πολυωνύμων.

Έστω $\mathbf{p}(\mathbf{x}) \in \mathbf{F}[\mathbf{x}]$ ανάγωγο πολυώνυμο. Το σώμα $\mathbf{F}[\mathbf{x}]/\langle \mathbf{p}(\mathbf{x}) \rangle$ περιέχει μία ρίζα του πολυωνύμου $\mathcal{F}(\mathbf{p}(\mathbf{x}))$.

$$\begin{aligned}
p(x) &= \Sigma_{k=0}^{n} p_k\, x^k, \\
\mathcal{F}(p(x)) = P(x) &= \Sigma_{k=0}^{n} f(p_k)\, x^k = \Sigma_{k=0}^{n} (p_k + \langle p(x) \rangle)\, x^k \Rightarrow \\
P(x + \langle p(x) \rangle) &= \Sigma_{k=0}^{n} (p_k + \langle p(x) \rangle) \odot (x + \langle p(x) \rangle)^k = \\
&= \Sigma_{k=0}^{n} (p_k + \langle p(x) \rangle) \odot (x^k + \langle p(x) \rangle) = \\
&= \Sigma_{k=0}^{n} ((p_k\, x^k) + \langle p(x) \rangle) = \\
&= \left(\Sigma_{k=0}^{n} p_k\, x^k \right) + \langle p(x) \rangle = \\
&= p(x) + \langle p(x) \rangle = \\
&= \{ p(x) + a(x)\, p(x) : a(x) \in F[x] \} = \\
&= \{ (1 + a(x))\, p(x) : a(x) \in F[x] \} = \\
&= \{ u(x)\, p(x) : u(x) \in F[x] \} = \langle p(x) \rangle = \\
&= 0 + \langle p(x) \rangle.
\end{aligned}$$

Άρα το στοιχείο $x + \langle p(x) \rangle$ του $F[x]/\langle p(x) \rangle$ είναι ρίζα του πολυωνύμου $P(x)$ δηλαδή του $\mathcal{F}(p(x))$.

$(*)$ **Για κάθε μη κενό σύνολο A υπάρχει ένα μη κενό σύνολο B ώστε τα στοιχεία του A να βρίσκονται σε ένα προς ένα και επί αντιστοιχία με τα στοιχεία του B.**

Θεωρούμε ένα στοιχείο b που δεν ανήκει στο σύνολο A. Το σύνολο,

$$B = \{b_a : \text{ για κάθε } a \in A\},$$

πληρεί την ζητούμενη προϋπόθεση.

Έστω $\mathbf{p(x) \in F[x]}$ ανάγωγο πολυώνυμο. Θεωρούμε το σύνολο $\mathbf{(F[x]/\langle p(x) \rangle) - FI}$. Θέτουμε EF ένα σύνολο του οποίου τα στοιχεία βρίσκονται σε ένα προς ένα και επί αντιστοιχία με αυτά του συνόλου $\mathbf{(F[x]/\langle p(x) \rangle) - FI}$. Από την $(*)$ ξέρουμε ότι το EF υπάρχει. Συμβολίζουμε με $\mathbf{\Phi}$ την ένα προς ένα και επί συνάρτηση από το EF στο $\mathbf{(F[x]/\langle p(x) \rangle) - FI}$ που εξασφαλίζει ότι τα στοιχεία των δύο συνόλων βρίσκονται σε ένα προς ένα και επί αντιστοιχία. Ορίζουμε την συνάρτηση $\mathfrak{F} : \mathbf{(EF \cup F) \mapsto F[x]/\langle p(x) \rangle}$,

$$\mathfrak{F}(\mathbf{a}) = \begin{cases} \mathbf{f(a)} & , \text{ όταν } \mathbf{a \in F}, \\ \mathbf{\Phi(a)} & , \text{ όταν } \mathbf{a \in EF}. \end{cases}$$

όπου f είναι η συνάρτηση που ορίσαμε από το $\mathbf{F} \mapsto \mathbf{FI}$. Είναι προφανές από τον ορισμό της ότι η $\mathfrak{F}$ είναι μία καλώς ορισμένη ένα προς ένα και επί συνάρτηση. Ορίζουμε πράξεις «πρόσθεσης» $\oplus$ και «πολλαπλασιασμού» $\odot$ στο $\mathbf{EF} \cup \mathbf{F}$ ως εξής,

$$\begin{aligned}
\mathbf{a} \oplus \mathbf{b} &= \mathfrak{F}^{-1}(\mathfrak{F}(\mathbf{a}) \oplus \mathfrak{F}(\mathbf{b})), \\
\mathbf{a} \odot \mathbf{b} &= \mathfrak{F}^{-1}(\mathfrak{F}(\mathbf{a}) \odot \mathfrak{F}(\mathbf{b})).
\end{aligned}$$

Όταν $\mathbf{a}, \mathbf{b} \in \mathbf{F}$ οι πιο πάνω ορισθείσες πράξεις είναι η πρόσθεση και ο πολλαπλασιασμός του σώματος $\mathbf{F}$ όπως φαίνεται από τις,

$$\begin{aligned}
\mathbf{a} \oplus \mathbf{b} &= \mathfrak{F}^{-1}(\mathfrak{F}(\mathbf{a}) \oplus \mathfrak{F}(\mathbf{b})) = \mathfrak{F}^{-1}(\mathbf{f}(\mathbf{a}) \oplus \mathbf{f}(\mathbf{b})) = \mathfrak{F}^{-1}(\mathbf{f}(\mathbf{a}+\mathbf{b})) = \\
&= \mathbf{f}^{-1}(\mathbf{f}(\mathbf{a}+\mathbf{b})) = \mathbf{a}+\mathbf{b}, \\
\mathbf{a} \odot \mathbf{b} &= \mathfrak{F}^{-1}(\mathfrak{F}(\mathbf{a}) \odot \mathfrak{F}(\mathbf{b})) = \mathfrak{F}^{-1}(\mathbf{f}(\mathbf{a}) \odot \mathbf{f}(\mathbf{b})) = \mathfrak{F}^{-1}(\mathbf{f}(\mathbf{a}\,\mathbf{b})) = \\
&= \mathbf{f}^{-1}(\mathbf{f}(\mathbf{a}\,\mathbf{b})) = \mathbf{a}\,\mathbf{b}.
\end{aligned}$$

Είναι άμεσο να επαληθευθεί ότι το $\mathbf{EF} \cup \mathbf{F}$ εφοδιασμένο με τις πιο πάνω ορισθείσες πράξεις είναι σώμα και η $\mathfrak{F}$ ένας ένα προς ένα και επί ομομορφισμός δηλαδή, ισομορφισμός μεταξύ των σωμάτων $\mathbf{EF} \cup \mathbf{F}$ και $\mathbf{F}[\mathbf{x}]/\langle \mathbf{p}(\mathbf{x}) \rangle$.

Γνωρίζουμε ότι το σώμα $F[x]/\langle p(x)\rangle$ περιέχει το στοιχείο $x+\langle p(x)\rangle$ που είναι μία ρίζα του $P(x)=\mathcal{F}(p(x))$. Επειδή το x δεν είναι σταθερό στοιχείο έπεται ότι το $x+\langle p(x)\rangle$ ανήκει στο $F[x]/\langle p(x)\rangle - FI$. Από τα πιο πάνω, υπάρχει στοιχείο $\rho=\Phi^{-1}(x+\langle p(x)\rangle)=\mathfrak{F}^{-1}(x+\langle p(x)\rangle)$ του $EF\subset(EF\cup F)$ ώστε αν $p(x)=\Sigma_{k=0}^{n}p_k\,x^k$ να λαμβάνουμε,

$$
\begin{aligned}
\mathfrak{F}(p(\rho)) &= \mathfrak{F}\left(\sum_{k=0}^{n} p_k\odot\rho^k\right)=\Sigma_{k=0}^{n}\mathfrak{F}(p_k)\odot\mathfrak{F}(\rho^k)=\\
&= \Sigma_{k=0}^{n}\mathfrak{F}(p_k)\odot\mathfrak{F}(\rho)^k=\Sigma_{k=0}^{n}f(p_k)\odot(x+\langle p(x)\rangle)^k=\\
&= \Sigma_{k=0}^{n}(p_k+\langle p(x)\rangle)\odot(x^k+\langle p(x)\rangle)=\\
&= \Sigma_{k=0}^{n}(p_k\,x^k+\langle p(x)\rangle)=\\
&= \left(\Sigma_{k=0}^{n}p_k\,x^k\right)+\langle p(x)\rangle=\\
&= p(x)+\langle p(x)\rangle=\\
&= \{p(x)+a(x)\,p(x):a(x)\in F[x]\}=\\
&= \{(1+a(x))\,p(x):a(x)\in F[x]\}=\\
&= \{u(x)\,p(x):u(x)\in F[x]\}=\langle p(x)\rangle=\\
&= 0+\langle p(x)\rangle.
\end{aligned}
$$

Όμως για το ουδέτερο στοιχείο της πρόσθεσης του σώματος $EF \cup F$ ισχύει, $\mathfrak{F}(0 \oplus 0) = \mathfrak{F}(0) \oplus \mathfrak{F}(0) = f(0) \oplus f(0) = (0 + \langle p(x) \rangle) \oplus (0 + \langle p(x) \rangle) = 0 + \langle p(x) \rangle$ δηλαδή, $\mathfrak{F}(0) = \mathfrak{F}(0 \oplus 0) = 0 + \langle p(x) \rangle$. Τελικώς, $\mathfrak{F}(p(\rho)) = 0 + \langle p(x) \rangle = \mathfrak{F}(0)$ και επειδή η $\mathfrak{F}$ είναι ένα προς ένα λαμβάνουμε $p(\rho) = 0$ επάγοντας ότι,

Για κάθε ανάγωγο πολυώνυμο $\mathbf{p(x)} \in \mathbf{F[x]}$ υπάρχει ένα σώμα $\mathbf{K} = \mathbf{EF} \cup \mathbf{F} \supseteq \mathbf{F}$ που περιέχει μία ρίζα του $\mathbf{p(x)}$.

Το τελευταίο συμπέρασμα επάγει ότι κάθε ανάγωγο πολυώνυμο έχει ρίζα όχι στο σώμα F στο οποίο ανήκουν οι συντελεστές του αλλά σε ένα ευρύτερο σώμα K του σώματος των συντελεστών και αυτή η ρίζα ανήκει στο $K - F$.

Έστω $\mathbf{p(x)} \in \mathbf{F[x]}$ ανάγωγο πολυώνυμο. Υπάρχει σώμα $\mathbf{K} \supseteq \mathbf{F}$ τέτοιο ώστε το $\mathbf{p(x)}$ να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $\mathbf{K[x]}$.

Εφαρμόζουμε επαγωγή στον βαθμό του $p(x)$. Αν $deg[p(x)] = 1$ τότε αυτό είναι πρωτοβάθμιο πολυώνυμο του $F[x]$ και το συμπέρασμα ισχύει για $K = F$. Υποθέτουμε ότι για κάθε $deg[p(x)] \leq n$ ότι το συμπέρασμα ισχύει. Έστω $deg[p(x)] = n+1$. Από την προηγούμενη ανάλυση υπάρχει σώμα $M \supseteq F$ που περιέχει μία ρίζα ρ του $p(x)$. Τότε,

$$p(x) = (x - \rho)\, q(x) + r(x),$$

με $q(x), r(x) \in M[x]$ και είτε $r(x) = 0$, είτε $0 = deg[r(x)] < deg[(x-\rho)] = 1$. Αν το $deg[r(x)] = 0$ το $r(x)$ είναι μη μηδενικό σταθερό πολυώνυμο του $M[x]$ δηλαδή, $p(x) = m \in M - \{0\}$. Επειδή $0 = p(\rho) = 0\, q(\rho) + r(\rho)$ έπεται $r(\rho) = 0$, άτοπο και το $r(x)$ δεν είναι μηδενικού βαθμού.
Άρα, $r(x) = 0$ και $p(x) = (x - \rho)\, q(x)$. Αν το $q(x)$ είναι ανάγωγο στο $M[x]$ και επειδή $deg[q(x)] = n$, από την υπόθεση της επαγωγής υπάρχει σώμα $K \supseteq M \supseteq F$ ώστε το $q(x)$ να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $K[x]$. Επειδή και $(x - \rho) \in M[x] \subseteq K[x]$, το $p(x)$ παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $K[x]$ και το συμπέρασμα προκύπτει. Αν το $q(x)$ δεν είναι ανάγωγο στο $M[x]$ τότε παραγοντοποιείται σε γινόμενο πολυωνύμων του $M[x]$ βαθμού μεγαλύτερου ή ίσου του 1 και αυτά εκ΄ νέου και ούτω καθ΄ εξής έως ότου προκύψουν παράγοντες του $M[x]$ που δεν μπορούν να παραγοντοποιηθούν περαιτέρω σε γινόμενο πολυωνύμων του $M[x]$ βαθμού μεγαλύτερου ή ίσου του 1.
Άρα μπορούμε να παραγοντοποιήσουμε το $q(x)$ σε γινόμενο ανάγωγων στο $M[x]$ πολυωνύμων του $M[x]$ βαθμού μικρότερου ή ίσου του βαθμού του $q(x)$. Έστω ότι αυτά είναι ν το πλήθος.

Για το i ανάγωγο πολυώνυμο, $i \in \{1, 2, \ldots, \nu\}$, από την υπόθεση της επαγωγής, υπάρχει σώμα $K_i \supseteq M \supseteq F$ ώστε αυτό να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων παραγόντων του $K_i[x]$. Οπότε, υπάρχει σώμα το $K = \cup_{i=1}^{\nu} K_i \supseteq M \supseteq F$ ώστε το γινόμενο των ν ανάγωγων πολυωνύμων να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $K[x]$. Επειδή και $(x - \rho) \in M[x] \subseteq K[x]$, το $p(x)$ παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $K[x]$ και το συμπέρασμα προκύπτει.

Έστω $\mathbf{a}(\mathbf{x}) \in \mathbf{F}[\mathbf{x}] - \{\mathbf{0}\}$. Υπάρχει σώμα $\mathbf{K} \supseteq \mathbf{F}$ τέτοιο ώστε το $\mathbf{a}(\mathbf{x})$ να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $\mathbf{K}[\mathbf{x}]$.

Αν το $a(x)$ είναι ανάγωγο στο $F[x]$ το συμπέρασμα προκύπτει από τα προηγούμενα. Αν το $a(x)$ δεν είναι ανάγωγο στο $F[x]$ τότε τότε παραγοντοποιείται σε γινόμενο πολυωνύμων του $F[x]$ βαθμού μεγαλύτερου ή ίσου του 1 και αυτά εκ΄ νέου και ούτω καθ΄ εξής έως ότου προκύψουν παράγοντες του $F[x]$ που δεν μπορούν να παραγοντοποιηθούν περαιτέρω σε γινόμενο πολυωνύμων του $F[x]$ βαθμού μεγαλύτερου ή ίσου του 1. Έστω ότι αυτά είναι ν το πλήθος. Για το i ανάγωγο πολυώνυμο, $i \in \{1, 2, \ldots, \nu\}$, από τα προηγούμενα υπάρχει σώμα $K_i \supseteq F$ ώστε αυτό να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων παραγόντων του $K_i[x]$. Οπότε, υπάρχει σώμα το $K = \cup_{i=1}^{\nu} K_i \supseteq F$ ώστε το γινόμενο των ν ανάγωγων πολυωνύμων να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $K[x]$ και το συμπέρασμα προκύπτει.

Έστω $\mathbf{a}(\mathbf{x}) \in \mathbf{F}[\mathbf{x}] - \{\mathbf{0}\}$, $\mathbf{K} \supseteq \mathbf{F}$ ένα σώμα στον δακτύλιο πολυωνύμων $\mathbf{K}[\mathbf{x}]$ του οποίου παραγοντοποιείται το $\mathbf{a}(\mathbf{x})$ σε γινόμενο πρωτοβάθμιων πολυωνύμων. Μπορούμε να γράψουμε,

$$\mathbf{a}(\mathbf{x}) = \mathbf{a_n}\,(\mathbf{x} - \mathbf{b_1})\,\cdots\,(\mathbf{x} - \mathbf{b_n}),$$

με $\mathbf{a_n} \in \mathbf{F} - \{\mathbf{0}\}$, $\mathbf{b_1}, \ldots, \mathbf{b_n} \in \mathbf{K}$.

Έστω $a(x) = \Sigma_{k=0}^{n}\, a_k\, x^k$. Επειδή το $a(x)$ έχει βαθμό n έπεται $a_n \neq 0$. Οπότε, $a(x) = a_n\, \Sigma_{k=0}^{n}(a_n^{-1}\, a_k)\, x^k = a_n\, \Sigma_{k=0}^{n}\, g_k\, x^k = a_n\, g(x)$ με $g_n = 1$, $g_k \in F$. Από τα προηγούμενα, υπάρχει σώμα $K \supseteq F$ ώστε το $g(x)$ να παραγοντοποιείται σε γινόμενο πρωτοβάθμιων πολυωνύμων του $K[x]$ έστω,

$$g(x) = (t_1\, x + h_1)\,(t_2\, x + h_2)\,\cdots\,(t_m\, x + h_m),$$

με $t_1, t_2, \ldots, t_m \in K - \{0\}$, $h_1, h_2, \ldots, h_m \in K$. Μπορούμε να γράψουμε,

$$\begin{aligned} g(x) &= (t_1\, t_2\, \cdots\, t_m)\,(x - (-t_1^{-1}\, h_1))\,(x - (-t_2^{-1}\, h_2))\,\cdots\,(x - (-t_m\, h_m)) = \\ &= t\,(x - b_1)\,(x - b_2)\,\cdots\,(x - b_m). \end{aligned}$$

Όμως ο συντελεστής του μεγιστοβάθμιου όρου του $g(x)$ ο $g_n = 1$ επάγει ότι $t = 1$ και τελικώς το $a(x)$ γράφεται,

$$a(x) = a_n\, g(x) = a_n\, (x - b_1) \cdots (x - b_n),$$

με $a_n \in F - \{0\}$, $b_1, \ldots, b_n \in K$.

Το συμπέρασμα που μόλις αποδείξαμε είναι γνωστό ως θεώρημα Girard–Kronecker. Το γνωστό μας Θεμελιώδες Θεώρημα της Άλγεβρας είναι εφαρμογή του θεωρήματοςGirard–Kronecker στην περίπτωση $F = \mathbb{C}$. Στην περίπτωση αυτή ο Gauss απέδειξε ότι και $K = \mathbb{C}$.

Το θεώρημα Girard–Kronecker εξασφαλίζει ότι το πλήθος των λύσεων, (όχι απαραιτήτως διακεκριμένων μεταξύ τους), της πολυωνυμικής εξίσωσης $a(x) = 0$ ισούται με τον βαθμό του πολυωνύμου $a(x)$. Αυτό που δεν εξασφαλίζει είναι ότι οι λύσεις αυτές είναι στοιχεία του σώματος F από το οποίο προέρχονται οι συντελεστές του πολυωνύμου $a(x)$. Μπορεί κάποιες ή όλες εξ' αυτών να ανήκουν στο F, μπορεί και όλες να είναι στοιχεία κάποιου σώματος K ευρύτερου του F.