ΠΕΡΙΕΧΟΜΕΝΑ

«Die Klassenkorpertheorie ist das Herzstuck der algebraischen Zahlentheorie und zweifellos eine den bedeutendsten Kulturleistungen des 20 Jahrhunderts.»

Helmut Koch 1987.

«He wrote to me that algebraic number theory was the most beautiful topic he had ever come across and that the sole consolation in misery was his lecturing on class field theory…

This was indeed the kind of mathematics he had admired most the main results are of great scope, of great aesthetic beauty, but the proofs are technically extremely hard.»

A.Borel about Harish-Chandra, 1995.

ΤΟ ΠΡΟΒΛΗΜΑ ΤΟΥ ΠΥΡΓΟΥ ΤΩΝ ΚΛΑΣΕΩΝ ΣΩΜΑΤΩΝ

ΕΙΣΑΓΩΓΗ

Στην εργασία αυτή ασχολούμαστε με το λεγόμενο πρόβλημα του πύργου των κλάσεων σωμάτων. Το πρόβλημα τέθηκε από τον Furtwangler και αναφέρεται στο Klassenkorperbericht του Hasse στα 1926 σε συνδυασμό με το, αναπόδεικτο τότε, θεώρημα των κυρίων διαιρετών. Η απάντηση στο πρόβλημα δόθηκε στα 1964 από τους Golod και Safarevich. Η απόδειξη που θα παρουσιάσουμε είναι του P. Roquette όπως αυτή αναφέρεται στο [CF]. Για κάπως διαφορετικές προσεγγίσεις στο θέμα παραπέμπουμε στα [H], [S] και [SH].

Για την διαπραγμάτευση του θέματος απαιτούνται γνώσεις αλγεβρικής θεωρίας αριθμών, θεωρίας ομάδων, συνομολογίας πεπερασμένων ομάδων καθώς και στοιχεία θεωρίας κλάσεων σωμάτων. Ήταν πρακτικά αδύνατο να συμπεριλάβουμε όλο αυτό το υλικό στην μεταπτυχιακή μας εργασία, αναφερόμαστε όμως εν συντομία στα δύο πρώτα κεφάλαια.

Το πρόβλημα τέθηκε ως εξής:

Μία από τις πιο σημαντικές διαφορές ανάμεσα στην αριθμητική των αλγεβρικών σωμάτων αριθμών K και στην αριθμητική του **Q** είναι ότι ο δακτύλιος των ακεραίων αλγεβρικών αριθμών του K δεν είναι για όλα τα σώματα K, δακτύλιος κυρίων ιδεωδών, όπως είναι το **Z**. Υπάρχουν δηλαδή αλγεβρικά σώματα αριθμών K με αριθμό κλάσεων ιδεωδών $h_K>1$. Εντελώς φυσιολογικά τίθεται το ερώτημα αν μπορεί το K να εμφυτευτεί σε κάποιο άλλο αλγεβρικό σώμα αριθμών L με αριθμό κλάσεων ιδεωδών $h_L=1$. Αν αυτό είναι δυνατόν τότε θα μπορούσαμε ίσως από το K να περάσουμε στο L να εργαστούμε πολύ πιο εύκολα σ΄ αυτό, λόγω του ότι $h_L=1$, και να «επιστρέψουμε» στο K. Το πρόβλημα αυτό θα λέγεται <u>πρόβλημα εμφύτευσης</u> του K και το L θα λέγεται <u>μια λύση</u> του προβλήματος εμφύτευσης. Έστω τώρα K_1 το <u>σώμα κλάσεων του Hilbert</u> του K. Το K_1 ορίζεται ως η <u>maximal, μη διακλαδιζόμενη</u> (ως προς όλους τους πρώτους πεπερασμένους και άπειρους) <u>αβελιανή</u> επέκταση του K. Από τη θεωρία κλάσεων σωμάτων είναι γνωστό ότι η ομάδα Galois της επέκτασης K_1 του K είναι ισόμορφη προς την ομάδα των κλάσεων ιδεωδών Cl_K του K. Επομένως $[K_1:K]=h_K$. Το θεώρημα των κυρίων διαιρετών ([N]) μας εξασφαλίζει ότι όλα τα ιδεώδη του K γίνονται <u>κύρια ιδεώδη</u> στο K_1. Αυτό βεβαίως <u>δεν</u> σημαίνει ότι όλα τα ιδεώδη του K_1 είναι κατ΄ανάγκη κύρια. Είναι κάλλιστα δυνατό να έχουμε $h_{K1}>1$. Σε αυτή την περίπτωση θεωρούμε το σώμα Hilbert K_2 του σώματος K_1. Συνεχίζοντας όμοια κατασκευάζουμε ένα πύργο σωμάτων

$$K \subseteq K_1 \subseteq K_2 \subseteq \dots$$

όπου το K_i για κάθε i=1,2,3… είναι το σώμα του Hilbert του K_{i-1}. Ο πύργος αυτός λέγεται πύργος των κλάσεων σωμάτων του K. Έστω $K_\infty = \bigcup_{i=1}^{\infty} K_i$. Το K_∞ είναι αλγεβρικό σώμα αριθμών το οποίο όμως είναι δυνατόν να είναι άπειρη επέκταση του **Q**. Στο Κεφάλαιο 3 θα αποδείξουμε ότι το πρόβλημα εμφύτευσης του K είναι ισοδύναμο με το πεπερασμένο του πύργου κλάσεων σωμάτων αυτού. Επομένως, αρκεί να μελετήσουμε τον πύργο κλάσεων σωμάτων. Το θεώρημα των Golod – Shafarevich μας δίνει ότι ο πύργος των κλάσεων δεν είναι πάντοτε πεπερασμένος.

ΚΕΦΑΛΑΙΟ 1

ΣΤΟΙΧΕΙΑ ΣΥΝΟΜΟΛΟΓΙΑΣ

Στο κεφάλαιο αυτό θα αναφερθούμε στα στοιχεία συνομολογίας πεπερασμένων ομάδων τα οποία είναι απαραίτητα για την απόδειξη του θεωρήματος του Shafarevich.
Πλήρη ανάπτυξη της θεωρίας με στόχο την συνομολογιακή παρουσίαση της θεωρίας κλάσεων σωμάτων (class field theory) μπορεί ο ενδιαφερόμενος αναγνώστης να βρει στο [W] ή στο [AW] που είναι μέρος του βιβλίου [CF].
Χρήσιμες για μια πιο εκτεταμένη εισαγωγή στη θεωρία συνομολογίας, από ότι είναι το παρόν κεφάλαιο, είναι και οι σημειώσεις [A1].

1.Ορισμός και ιδιότητες

Ορισμός1.1

Έστω G πεπερασμένη ομάδα. Μια αβελιανή (προσθετικά) ομάδα A θα λέγεται G-module όταν η G δρα επί της A και ισχύουν :

(i)$1\alpha=\alpha$ για κάθε $\alpha\in A$

(ii)$\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$ για κάθε $\alpha,\beta\in A$ και $\sigma\in G$

(iii)$\sigma(\tau\alpha)=(\sigma\tau)(\alpha)$ για κάθε $\alpha\in A$ και $\sigma,\tau\in G$.

Ορισμός 1.2

Σε κάθε πεπερασμένη ομάδα G ορίζεται ο δακτύλιος ομάδας

$$\mathbf{Z[G]=\{\sum_{\sigma\in G} n_\sigma\sigma \ / \ n_\sigma\in Z\}.}$$

Το Z[G] είναι ελεύθερη αβελιανή ομάδα παραγόμενη από τα στοιχεία της G. Η πρόσθεση των στοιχείων της Z[G] ορίζεται ως εξής :

$$\mathbf{\sum_{\sigma\in G} n_\sigma\sigma+\sum_{\sigma\in G} m_\sigma\sigma=\sum_{\sigma\in G}(n_\sigma+m_\sigma)\sigma.}$$

Αν ορίσουμε και τον πολαπλασιασμό :

$$\mathbf{(\sum_{\sigma\in G} n_\sigma\sigma)(\sum_{\sigma\in G} m_\sigma\sigma)=\sum_{\sigma\in G}(\sum_{\tau\rho=\sigma} n_\sigma n_\rho)\sigma,}$$

τότε το Z[G] γίνεται δακτύλιος και λέγεται δακτύλιος ομάδας της G.

Παρατήρηση 1.3

Εύκολα διαπιστώνουμε οτι η έννοια του G-module ταυτίζεται με την συνηθισμένη έννοια του Z[G]-module. Το Z[G] είναι, ως προσθετική ομάδα, επίσης ένα G-module.

Ο δακτύλιος των ακεραίων Z είναι πάντοτε G-module ως προς κάθε πεπερασμένη ομάδα G με τετριμμένη δράση. Ομοίως το Q και η ομάδα πηλίκων Q/Z.

Θεωρούμε την απεικόνιση,

$$\varepsilon : \mathbf{Z}[G] \to \mathbf{Z}, \text{ όπου } \varepsilon(\sum_{\sigma\in G} n_\sigma\sigma = \sum_{\sigma\in G} n_\sigma).$$

Εύκολα διαπιστώνουμε οτι η ε είναι ομομορφισμός δακτυλίων.
Ο πυρήνας του ομομορφισμού της ε

$$I_G:=\{ \sum_{\sigma\in G} n_\sigma\sigma \ / \sum_{\sigma\in G} n_\sigma\sigma =0\}$$

είναι ως γνωστό, ένα ιδεώδες του **Z**[G] και λέγεται augmentation ιδεώδες του **Z**[G].
Αν A, B είναι G-modules τότε με Hom(A,B) θα συμβολίζουμε την ομάδα των ομομορφισμών ομάδων $f : A \to B$.

Ορισμός 1.4
Ο ομομορφισμός $f : A \to B$ θα λέγεται G-ομομορφισμός αν, επί πλέον, ισχύει $f(\sigma a)=\sigma f(a)$ για κάθε $\sigma\in G$ και για κάθε $a\in A$.

Το σύνολο των G-ομομορφισμών $f : A \to B$ αποτελεί υποομάδα της ομάδας Hom(A,B) και συμβολίζεται με $Hom_G(A,B)$. Η ομάδα των ομομορφισμών Hom(A,B) γίνεται G-module με δράση

$$\sigma(f)=\sigma f\sigma^{-1}.$$

Σε κάθε G-module A ορίζουμε το σύνολο

$$A^G:=\{a\in A/\sigma(a)=a, \text{ για κάθε } \sigma\in G\}.$$

Εύκολα διαπιστώνουμε ότι το A^G είναι ένα G-module και μάλιστα το μέγιστο υπομodule του A στο οποίο η G δρα τετριμμένα και θα λέγεται η ομάδα των σταθερών στοιχείων της A.
Με N_G θα συμβολίζουμε το στοιχείο $N_G=\sum_{\sigma\in G} \sigma$ της **Z**[G]. Η απεικόνιση

$$\mu : \mathbf{Z} \to \mathbf{Z}[G], \text{ όπου } \mu(n)=nN_G \text{ για κάθε } n\in \mathbf{Z}$$

είναι επίσης ομομορφισμός ομάδων.

Παρατήρηση 1.5
(i)Σύμφωνα με τα παραπάνω, έχουμε

$$\mathbf{Hom_G(A,B)=(Hom(A,B))^G}$$

και ειδικά :

$$\mathbf{Hom_G(Z,A)=(Hom(Z,A))^G=A^G.}$$

(ii)Επειδή ο τελεστής Hom είναι αριστερά ακριβής (δες, [A1]) έπεται ότι, αν η

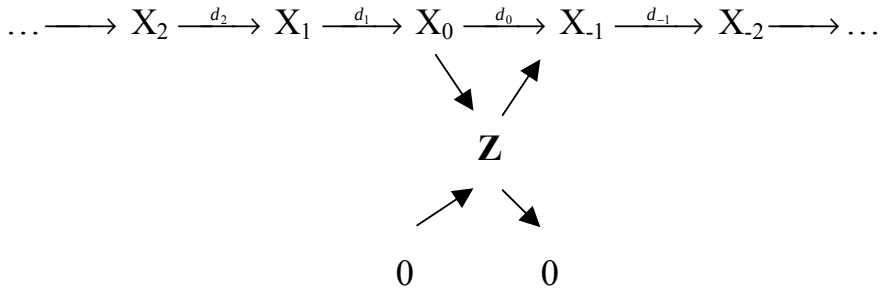
$$\mathbf{0 \to A \to B \to C \to 0}$$

είναι ακριβής ακολουθία από G-modules, τότε η

$$\mathbf{0} \to \mathbf{A^G} \to \mathbf{B^G} \to \mathbf{C^G} \to \mathbf{0}$$

είναι μία ακριβής ακολουθία αβελιανών ομάδων.

Έστω τώρα G μία πεπερασμένη ομάδα.
Μία <u>πλήρης ελεύθερη επίλυση (resolution) της ομάδας G</u> (ή του G-module **Z**, όπου η δράση της G στον **Z** είναι τετριμμένη, δηλαδή σm=m για κάθε σ∈ G) είναι το εξής (complex):



όπου ε : $X_0 \to \mathbf{Z}$ και μ : $\mathbf{Z} \to X_{-1}$
με τις παρακάτω ιδιότητες :
(i) X_q είναι ελεύθερο G-module για κάθε q∈ **Z**
(ii) ε,μ,d_q είναι G-ομομορφισμοί, για κάθε q∈ **Z**
(iii) $d_0=\mu\circ\varepsilon$
(iv) έχουμε ακρίβεια της ακολουθίας σε κάθε θέση.

Η απάντηση στο ερώτημα αν κάθε ομάδα G επιδέχεται μία τέτοια επίλυση είναι θετική. Επιδέχεται τουλάχιστο την <u>standard επίλυση</u> η οποία έχει το πρότυπο της στην αλγεβρική τοπολογία.
Για κάθε q≥1 ορίζουμε τα σύμβολα

$[\sigma_1,\sigma_2,\ldots,\sigma_q]$ / $\sigma_i\in$ G (q-κυψελίδες)

και τα χρησιμοποιούμε σαν <u>ελεύθερους γεννήτορες</u> των G-modules μας. Θέτουμε

$$X_q=X_{-q-1}=\sum\oplus \mathbf{Z}[\sigma_1,\sigma_2,\ldots\sigma_q]$$

(τα $X_q=X_{-q-1}$ παράγονται σαν ελεύθερα **Z**-module από $\sigma[\sigma_1,\sigma_2,\ldots,\sigma_q]$ / σ, $\sigma_i\in$ G).
$X_0=X_{-1}=\mathbf{Z}[G]$ είναι το ελεύθερο G-module που παράγεται από τα στοιχεία της G (σαν **Z**-module).

$\varepsilon : \mathbf{Z}[G] \to \mathbf{Z}$, όπου $\varepsilon(\sum_{\sigma\in G} n_\sigma\sigma)= \sum_{\sigma\in G} n_\sigma$

$\mu(n)=nN_G$

$d_1([\sigma])=\sigma[\sigma]-[\sigma]$

$$d_n([\sigma_1,\ldots,\sigma_q])=\sigma_1[\sigma_2,\ldots,\sigma_q]+\sum_{i=1}^{q-1}(-1)^i[\sigma_1,\sigma_2,\ldots,\sigma_{i-1},\sigma_i.\sigma_{i+1},\ldots,\sigma_q]$$
$$+(-1)^n[\sigma_1,\sigma_2,\ldots,\sigma_{q-1}]\ n\geq 1.$$
$$d_{-1}([.])=\sum_{\sigma\in G}(\sigma_{-1}[\sigma]-[\sigma])$$
$$d_{-q-1}([\sigma_1,\ldots,\sigma_q]=\sum_{\sigma\in G}\sigma_1[\sigma,\sigma_1,\ldots,\sigma_q]+\sum_{\sigma\in G}\sum_{i=1}^{q}(-1)^i[\sigma_1[\sigma_1,\ldots,\sigma_{i-1},\sigma_i,\sigma_{i+1},\ldots,\sigma_q]+$$
$$\sum_{\sigma\in G}(-1)^{q+1}[\sigma_1,\sigma_2,\ldots,\sigma_q,\sigma],\ q>1.$$

<u>Θεώρημα 1.6</u>
Τα παραπάνω είναι μία πλήρης ελεύθερη ανάλυση της ομάδας G.
<u>Απόδειξη</u>
Δες, [W], Th.1.3.1 και Th.1.4.1, σελίδες 14,18.

Έστω τώρα A ένα G-module. Για κάθε $q\in\mathbf{Z}$, ορίζουμε την q-αλυσίδα
$$A_q:=\mathrm{Hom}_G(X_q,A)=\{f: X_q\to A \,/\, f,\ \text{G-ομομορφισμός}\}$$
τις <u>q-αλυσίδες του A</u>.
Η ακριβής ακολουθία
$$\ldots\longrightarrow X_2\xrightarrow{d_2}X_1\xrightarrow{d_1}X_0\xrightarrow{d_0}X_{-1}\xrightarrow{d_{-1}}X_{-2}\longrightarrow\ldots$$
επάγει την, εν γένει μη ακριβή, ακολουθία
$$\ldots\xrightarrow{\partial_{-1}}A_{-1}\xrightarrow{\partial_0}A_0\xrightarrow{\partial_1}A_1\longrightarrow\ldots$$
όπου $(\partial_{q+1}\,o\,\partial_q)(\varphi)=\partial_{q+1}(\partial_q(\varphi))=\partial_{q+1}(\varphi\,o\,d_q)=\varphi\,o\,d_q\,o\,d_{q+1}=\varphi\,o\,0=0$.
Άρα $\mathrm{Im}(\partial_q)\subseteq\mathrm{Ker}\,\partial_{q+1}$ οπότε ορίζουμε
$Z_q=\mathrm{Ker}\,\partial_{q+1}$ τους <u>q-συνκύκλους</u> (q-cocycles)
$B_q=\mathrm{Im}\,\partial_q$ τα <u>q-συνσύνορα</u> (q-cocboyndary)
και $H^q(G,A)=Z_q/B_q=$<u>q-ομάδα συνομολογίας με συντελεστές στο A</u>.
Αποδεικνύεται ότι οι ομάδες συνομολογίας $H^q(G,A)$ είναι ανεξάρτητες από την επίλυση (complex) (δές, [W], Prop.2.2.1, σελ.55).
Το X_q παράγεται ελεύθερα από q-κυψελίδες $[\sigma_1,\ldots\sigma_q]$ του καρτεσιανού γινομένου. Η f ορίζεται από τις τιμές στις q-κυψελίδες. Άρα η f μπορεί να θεωρηθεί σαν συνάρτηση
$$f: G\times G\times\ldots\times G\to A.$$
(q φορές)
Λόγω του ορισμού των d_q οι ∂_q ορίζονται ως εξής :
$$\partial_q\alpha=d_0=N_G\alpha$$
$$(\partial_1\alpha)([\sigma])=\sigma\alpha-\alpha$$

$$\partial_q f([\sigma_1,\ldots,\sigma_q])=\sigma_1 f([\sigma_2,\ldots,\sigma_q])+$$

$$+\sum_{\varepsilon=1}^{q-1} (-1)^i f([\sigma_1,\sigma_2,\ldots,\sigma_{i-1},\sigma_i,\sigma_{i+1},\ldots,\sigma_q])$$
$$+(-1)^n f([\sigma_1,\sigma_2,\ldots,\sigma_{q-1}]) \ ,f\in A_{q-1},\ q\geq 1$$

$$\partial_{-1} f=\sum_{\sigma\in G} (\sigma^{-1}[\sigma]-f[\sigma])$$

$$(\partial_{-q-1} f)([\sigma_1,\ldots,\sigma_q])=\sum_{\sigma\in G} \sigma^1 f([\sigma,\sigma_1,\ldots,\sigma_q])+$$
$$+\sum_{\sigma\in G}\sum_{i=1}^{q} (1)^i f([\sigma_1[\sigma_1,\ldots,\sigma_{i1},\sigma_i,\sigma_{i+1},\ldots,\sigma_q])+$$
$$+\sum_{\sigma\in G} (-1)^{q+1} f([\sigma_1,\sigma_2,\ldots \ ,\sigma_q,\sigma]),\ q\geq 0,\ x\in A_{-q-2}.$$

2.Υπολογισμός ομάδων συνομολογίας χαμηλής διάστασης

Συμβολισμοί : $A^G:=\{\alpha\in A \,/\, \sigma(\alpha)=\alpha,\ \text{για κάθε } \sigma\in G\}$

$$N_G:=\sum_{\sigma\in G} \sigma \in \mathbf{Z}[G]$$

$$N_G A:=\{N_G\,\alpha=\sum_{\sigma\in G} \alpha/\ \alpha\in A\}$$

$$NA:=\{\alpha\in A/N_G\alpha=0\}.$$

Πρόταση 2.1

Ισχύει :

$$\mathbf{H^0(G,A)=A^G/N_GA.}$$

Απόδειξη

Γνωρίζουμε ότι $H^0(G,A)=Z_0/R_0$ όπου $Z_0=Ker(\partial_1)=$

$$=\{f\in A \,/\, \sigma f-f=0 \text{ για κάθε } \sigma\in G\}=$$
$$=\{f\in A \,/\, \sigma f=f \text{ για κάθε } \sigma\in G\}=A^G$$
$$R_0=Im\,\partial_0=\{\alpha\in A \,/\, \text{υπάρχει } \alpha\in A,\ N_G\alpha'=\alpha\}$$
$$=N_GA.$$

Πόρισμα 2.2

Αν η G έχει τάξη n και δρα τετριμμένα επί της A τότε: $H^0(G,A)=A/nA$.
Ιδιαίτερα $H^0(G,Z)=Z/nZ$.
Αν L/K επέκταση του Galois, με G=G(L/K) τότε $H^0(G,L^*)=K^*/N_{L/K}L^*$.

Απόδειξη

Το K είναι το σώμα σταθερών στοιχείων της G, $(L^*)^G=K^*$ και επειδή το module L^* είναι πολλαπλασιαστικό έχουμε

$$N_G L^*=\{\prod_{\sigma\in G} \sigma(\alpha)/\alpha\in L^*\}=N_{L/K}L^*.$$

Πρόταση 2.3

Ισχύει :

$H^1(G,A)$={σταυρωτοί ομομορφισμοί}/{κύριους σταυρωτούς ομομορφισμούς}

Απόδειξη

Γνωρίζουμε οτι $H^1(G,A)=Z_1/R_1$, όπου

$Z_1=\mathrm{Ker}\,\partial_2=\{f : G\to A / \partial_2 f=0\}$

$=\{ f : G\to A / \sigma f(\tau)-f(\sigma\tau)+f(\sigma)=0$ για κάθε $\sigma,\tau\in G\}$

$=\{ f : G\to A / f(\sigma\tau)=\sigma f(\tau)+f(\sigma)$ για κάθε $\sigma,\tau\in G\}$

$=\{ f : G\to A / f$ σταυρωτός ομομορφισμός$\}$

$B_1=\mathrm{Im}\,\partial_1=\{ f : G\to A /$ υπάρχει $\alpha\in A$ $\partial_1\alpha=f(\sigma)$ για κάθε $\sigma\in G\}$

$=\{ f : G\to A / f(\sigma)=\sigma\alpha-\alpha$,με σταθερό $\alpha\in G$ για κάθε $\sigma\in G\}$

$=\{ f : G\to A / f$ κύριος σταυρωτός ομομορφισμός$\}$.

Έστω G΄ η ομάδα χαρακτήρων της G, $G'=\mathrm{Hom}(G,\mathbf{Q}/\mathbf{Z})$.

Αν η G δρα τετριμμένα επί του A τότε,

$$H^1(G,A)=\mathrm{Hom}(G,A)$$

διότι ο σταυρωτός ομομορφισμός είναι ομομορφισμός ομάδων, δηλαδή $f(\sigma\tau)=f(\sigma)+f(\tau)$, για κάθε $\sigma,\tau\in G$ ενώ ο μοναδικός κύριος σταυρωτός ομομορφισμός είναι ο τετριμμένος $f(\sigma)=0$ για κάθε $\sigma\in G$. Ιδιαίτερα για $A=\mathbf{Q}/\mathbf{Z}$ έχουμε :

$H^1(G,\mathbf{Q}/\mathbf{Z})=\mathrm{Hom}(G,\mathbf{Q}/\mathbf{Z})=G'\cong G/[G,G]$, όπου [G,G] η ομάδα των μεταθετών της G.

Θεώρημα 2.4

Αν L/K είναι πεπερασμένη επέκταση του Galois και G=G(L/K), τότε $H^1(G,L^*)=1$.

Απόδειξη

Η L^* είναι πολλαπλασιαστική ομάδα. Ισχύει

$$f\in Z_1 \Leftrightarrow f(\sigma\tau)=(\sigma f(\tau))f(\sigma) \text{ για κάθε } \sigma,\tau\in G.$$

Για κάθε $\beta\in L^*$, σχηματίζουμε το άθροισμα $\gamma(\beta):=\sum_{\tau\in G} f(\tau)\tau(\beta)$.

Αν όλα αυτά τα αθροίσματα $\gamma(\beta)$ ήταν ίσα με 0, για κάθε $\beta\in L^*$, τότε (επειδή οι αυτομορφισμοί τ είναι γραμμικά ανεξάρτητοι) έχουμε ότι $f(\tau)=0$ για κάθε $\tau\in G$. Επομένως υπάρχει $\beta\in L^*$ τέτοιο ώστε :

$$\gamma=\sum_{\tau\in G} f(\tau)\tau(\beta)\neq 0.$$

Επομένως, για κάθε $\sigma\in G$, ισχύει :

$$\sigma\gamma=\sum_{\tau\in G}(\sigma f(\tau)(\sigma\tau(\beta))=\sum_{\tau\in G}(f(\sigma\tau)/f(\sigma))(\sigma\tau)(\beta)$$

και επομένως $(\sigma\gamma)f(\sigma)=\sum_{\tau\in G} f(\sigma\tau)(\sigma\tau(\beta))=\gamma$,

οπότε $f(\sigma)=\gamma/\gamma\sigma=\sigma\gamma^{-1}/\gamma^{-1}$, δηλαδή $f\in B_1$. Αποδείξαμε επομένως ότι $Z_1=B_1$, δηλαδή ότι $H^1(G,L^*)=Z_1/B_1=1$.

Πόρισμα 2.5 (Θεώρημα 90 του Hilbert)

Έστω L/K κυκλική επέκταση βαθμού n και $G=G(L/K)=<\sigma>$. Αν $\alpha\in L$: $N_{L/K}(\alpha)=1$ τότε υπάρχει $\beta\in L^*$ τέτοιο ώστε $\alpha=\sigma(\beta)/\beta$.

Απόδειξη

Ορίζουμε την απεικόνιση $f : G\to L^*$ όπου $f(1)=1$, $f(\sigma)=\alpha$, $f(\sigma^2)=\alpha(\sigma(\alpha))$, … ,
$f(\sigma^{n-1})=\alpha(\sigma\alpha)\ldots(\sigma^{n-2}\alpha)$

Ισχύει $f(\sigma^\kappa\sigma^\lambda)=\sigma^\kappa f(\sigma^\lambda)f(\sigma^\kappa)$, δηλαδή η απεικόνιση είναι 1-κύκλος.

Αλλά $H^1(G,L^*)=1$, άρα η f είναι 1-σύνορο, $f\in B_1$ οπότε υπάρχει $\beta\in L^*$ με $f(\sigma)=\sigma(\beta)/\beta$ και επομένως $\alpha=f(\sigma)=\sigma(\beta)/\beta$.

Θεώρημα 2.6

Αν $0\longrightarrow A\xrightarrow{i} B\xrightarrow{j} C\longrightarrow 0$ είναι ακριβής ακολουθία από G-modules και G-ομομορφισμούς, τότε η αντίστοιχη ακολουθία των ομάδων συνομολογίας
$\ldots\longrightarrow H^n(G,A)\xrightarrow{i_*} H^n(G,B)\xrightarrow{j_*} H^n(G,C)\xrightarrow{\delta_*} H^{n+1}(G,A)\longrightarrow\ldots$
(όπου δ_* ο λεγόμενος συνδετικός ομομορφισμός) είναι επίσης ακριβής.

Απόδειξη

Δες, [W], Prop.2.2.4, σελίδα 57.

3.Πηλίκο του Herbrand

Στην παράγραφο αυτή υποθέτουμε ότι η G είναι μία κυκλική ομάδα τάξης n και A ένα G-module. Με $h_q(A)$ θα συμβολίζουμε την τάξη της ομάδας συνομολογίας $H^q(G,A)$ $q=0,1,\ldots$ υπό την προϋπόθεση ότι αυτή η ομάδα συνομολογίας είναι πεπερασμένη.

Αν λοιπόν οι ομάδες $H^0(G,A)$ και $H^1(G,A)$ είναι πεπερασμένες τότε το πηλίκο του Herbrand ορίζεται ως εξής

$$h(A):=h_0(A)/h_1(A).$$

Πρόταση 3.1

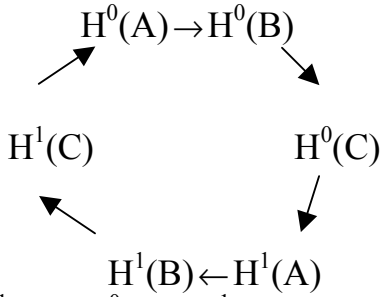
Αν G είναι μια κυκλική πεπερασμένη ομάδα και A ένα G-module τότε
$H^q(G,A)= H^{q+2}(G,A)$.

Απόδειξη
Δες, [W], Prop.3.2.1, σελίδα 93.

Πρόταση 3.2
Έστω $0 \to A \to B \to C \to 0$ μία ακριβής ακολουθία από G-modules (η G είναι κυκλική ομάδα). Τότε αν τα δύο από τα πηλίκα του Herbrand h(A), h(B), h(C) ορίζονται τότε ορίζεται και το τρίτο και μάλιστα ισχύει

$h(B)=h(A)h(C)$.

Απόδειξη
Λόγω της περιοδικότητας των ομάδων συνομολογίας $H^q(G,A)$ (πρόταση 2.1) η μακρά ακριβής συνομολογιακή ακολουθία γίνεται ένα ακριβές εξάγωνο, όπου $H^q(A)$ σημαίνει $H^q(G,A)$ για κάθε G-module A. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι τα πηλίκα h(A), h(B) ορίζονται. Θα αποδείξουμε ότι ορίζεται και το h(C) και μάλιστα h(C)=h(A)h(B).
Επειδή $0 \to A \to B \to C \to 0$ έχουμε οτι η παρακάτω ακολουθία είναι ακριβής



Υποθέτουμε οτι οι $H^0(A)$, $H^1(A)$, $H^0(B)$, $H^1(B)$ είναι πεπερασμένες. Έστω M_1 η εικόνα της $H^0(A)$ μέσα στην $H^0(B)$, M_2 η εικόνα της $H^0(B)$ μέσα στο $H^0(C)$ κ.ο.κ σαρώνοντας το εξάγωνο κατά την φορά των δεικτών του ρολογιού. Τότε η ακολουθία

$$0 \to M_2 \to H^0(C) \to M_3 \to 0$$

είναι ακριβής και τα M_2 και τα M_3 είναι πεπερασμένες ομάδες (η M_2 διότι είναι ομομορφική εικόνα της $H^0(B)$ η M_3 επειδή είναι υποομάδα της $H^1(A)$). Οπότε $H^0(C)$ είναι πεπερασμένη και όμοια και η $H^1(C)$ είναι πεπερασμένη. Δηλαδή ορίζεται το πηλίκο του Herbrand h(C). Η τάξη των ομάδων $H^0(A)$, $H^0(B)$, $H^0(C)$, $H^1(A)$, $H^1(B)$, $H^1(C)$ είναι αντίστιχα m_6m_1, m_1m_2, …, m_5m_6 όπου m_i η τάξη της M_i οπότε h(B)=h(A)h(C).

4.Η ακολουθία Restriction–Inflation

Έστω G και G΄ δύο πεπερασμένες ομάδες και A ένα G-module. Αν $f : G' \to G$ είναι ομομορφισμός ομάδων, τότε το G-module A γίνεται και G΄-module όπου η δράση της G΄ στο A ορίζεται μέσω της f,

$$g'(\alpha) := f(g')\alpha.$$

Επομένως η f επάγει έναν ομομορφισμό μεταξύ των ομάδων συνομολογίας

$$f^* : H^q(G,A) \to H^q(G',A).$$

Αν τώρα θεωρήσουμε την ειδική περίπτωση όπου η G΄=H είναι υποομάδα της G και η f είναι η εμφύτευση της H στην G τότε η επαγώμενη απεικόνιση μεταξύ των ομάδων συνομολογίας λέγεται <u>περιορισμός</u> (restriction)και συμβολίζεται, $Res : H^q(G,A) \to H^q(H,A)$.

Αν, επιπλέον, η ομάδα H είναι κανονική υποομάδα της G και σαν ομομορφισμό f θεωρήσουμε την προβολή της G στην ομάδα πηλίκων της G/H τότε παρατηρούμε ότι η υποομάδα A^H της A, που είναι η υποομάδα των σταθερών στοιχείων του A μέσω της δράσης της H, γίνεται G/H-module με δράση $(gH)\alpha = g\alpha$ για κάθε $\alpha \in A^H$ και συνεπώς επάγει έναν ομομορφισμό μεταξύ των ομάδων συνομολογίας $H^q(G/H,A^H)$ και $H^q(G,A)$ ο οποίος λέγεται <u>πληθωρισμός</u> (inflation) και συμβολίζεται με

$$Inf : H^q(G/H,A^H) \to H^q(G,A).$$

<u>Θεώρημα 4.1</u>

Έστω H μια κανονική υποομάδα της G και A ένα G-module. Τότε η παρακάτω ακολουθία είναι ακριβής

$$\mathbf{0 \to H^1(G/H,A^H) \to H^1(G,A) \to H^1(H,A).}$$

<u>Απόδειξη</u>

Δες, [CF], Prop.4, σελίδα 100 .

<u>Σημείωση 4.2</u>

Αν ισχύει επιπλέον ότι $H^i(H,A)=0$ για κάθε i, $1 \le i \le q-1$ όπου $q \in N$ τότε η ακολουθία $0 \to H^1(G/H,A^H) \xrightarrow{inf} H^1(G,A) \xrightarrow{Res} H^1(H,A) \to 0$ είναι ακριβής.

<u>Απόδειξη</u>

Δες, [CF], Prop.5, σελίδα 101.

5. Τετριμμένη Συνομολογία

Ορισμός 5.1
Ένα G-module A λέγεται συνομολογιακά τετριμμένο αν για κάθε υποομάδα H της G η $H^q(H,A)=0$ για όλους τους ακεραίους q.

Λήμμα 5.2
Έστω p ένας πρώτος αριθμός, G μια p-ομάδα και A ένα G-module τέτοιο ώστε pA=0. Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες :
(i) A=0
(ii) $H^0(G,A)=0$
(iii) $H_0(G,A)=0$.
Απόδειξη
Δες, [CF], Lemma 1, σελίδα 111.

Λήμμα 5.3
Έστω p ένας πρώτος αριθμός, G μια p ομάδα A ένα G-module τέτοιο ώστε pA=0 και $H^1(G,A)=0$. Τότε το A είναι ένα ελεύθερο module πάνω από το $F[G]=\Lambda/p\Lambda$.
Απόδειξη
Δες, [CF], Lemma 2, σελίδα 111.

Θεώρημα 5.4
Έστω G μία p-ομάδα και έστω A ένα G –module τέτοιο ώστε pA=0. Τότε οι παρακάτω προτάσεις είναι ισοδύναμες :
(i) το A είναι ένα ελεύθερο $F_p[G]$-module
(ii) το A είναι συνομολογιακά τετριμμένο
(iii) $H^q(G,A)=0$ για κάθε ακέραιο q.
Απόδειξη
Δες, [CF], Th.6, σελίδα 112.

Θεώρημα 5.5
Έστω G μια p-ομάδα και A ένα G-module χωρίς p-torsion. Τότε οι παρακάτω προτάσεις είναι ισοδύναμες :
(i) το A είναι συνομολογιακά τετριμμένο
(ii) $H^q(G,A)=H^{q+1}(G,A)=0$ για κάποιο ακέραιο q
(iii) το A/pA είναι ένα ελεύθερο $F_p[G]$-module.
Απόδειξη
Η συνεπαγωγή από το (i) στο (ii) είναι προφανής.

Από την (ii) στην (iii) έχουμε :
Επειδή η ακολουθία

$$0 \longrightarrow A \longrightarrow A \longrightarrow A/pA \longrightarrow 0$$

είναι ακριβής, προκύπτει ότι και η παρακάτω ακολουθία είναι ακριβής

$$H^q(G,A) \longrightarrow H^{q+1}(G,A/pA) \longrightarrow H^{q+1}(G,A).$$

Οπότε από το Θεώρημα 4.4 έπεται οτι το A/pA είναι ελεύθερο $F_p[G]$-module, δηλαδή η (iii).
Από το (iii) στο (i) έχουμε :
Από την ίδια ακριβή ακολουθία προκύπτει ότι η απεικόνιση

$$p : H^q(G,A) \longrightarrow H^q(G,A)$$

είναι ισομορφισμός για όλους τους ακεραίους q και όλες τις υποομάδες H της G. Αλλά $H^q(G,A)$ είναι μια p-ομάδα οπότε $H^q(G,A)=0$.

Πόρισμα 5.6
Έστω A ένα G-module το οποίο είναι Z-free και ικανοποιεί τις προϋποθέσεις του προηγούμενου θεωρήματος. Τότε για κάθε torsion free G-module B το G-module N=Hom(A,B) είναι συνομολογιακά τετριμμένο.
Απόδειξη
Δες, [CF], Cor. σελίδα 112.

6. Θεώρημα του Tate

Θεώρημα 6.1
Έστω A ένα G-module και $\alpha \in H^2(G,A)$. Για κάθε p πρώτο έστω G_p μια Sylow p-υποομάδα της G και υποθέτουμε ότι
(i)$H^1(G_p,A)=0$
(ii)$H^2(G_p,A)$ γεννάται από $Res_{G/Gp}(\alpha)$ και έχει τάξη ίση με την τάξη της G_p.
Τότε για όλες τις υποομάδες H της G και για κάθε ακέραιο n ισχύει

$$H^n(H,Z) \cong H^{n+2}(H,A).$$

Απόδειξη
Δες, [CF], Th.12, σελίδα 115.

ΚΕΦΑΛΑΙΟ 2

ΣΤΟΙΧΕΙΑ ΑΛΓΕΒΡΙΚΗΣ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

1. Εισαγωγικά

Ορισμός 1.1
Κάθε πεπερασμένη επέκταση του Q η οποία περιέχεται στο σώμα των μιγαδικών αριθμών C θα λέγεται αλγεβρικό σώμα αριθμών .
παραδείγματα
Q(i), Q($\sqrt{2}$),…

Ορισμός 1.2
Ένας μιγαδικός αριθμός θ λέγεται ακέραιος αλγεβρικός αν υπάρχει ένα μονικό πολυώνυμο p(t) με ακέραιους συντελεστές το οποίο να έχει ρίζα το θ, δηλαδή τέτοιο ώστε p(θ)=0.

Εαν τώρα θεωρήσουμε ένα αλγεβρικό σώμα αριθμών, το σύνολο των ακεραίων αλγεβρικών του K,

$$R_K=\{\alpha\in K \,/\, \alpha \text{ είναι ακέραιος αλγεβρικός}\}$$

αποτελεί **δακτύλιο**, υποδακτύλιο του K. Σαν υποδακτύλιος σώματος είναι ακέραια περιοχή της οποίας μάλιστα το K είναι το σώμα πηλίκων αυτής.

Στο κεφάλαιο αυτό περιγράφουμε βασικές έννοιες και θεωρήματα αλγεβρικής θεωρίας αριθμών τα οποία μας είναι απαραίτητα στην απόδειξη του θεωρήματος του Shafarevich. Για τις αποδείξεις των αυτών των αποτελεσμάτων παραπέμπουμε στα [A2], [ST], [CF], [N1].

Βασικό «μειονέκτημα» του δακτυλίου R_K είναι ότι δεν είναι πάντοτε δακτύλιος μονοσήμαντης ανάλυσης όπως των ακεραίων **Z**, π.χ. για K=**Q**($\sqrt{-5}$), ο δακτύλιος των ακεραίων αλγεβρικών είναι **Z**[(1+$\sqrt{-5}$)/2] ο οποίος δεν είναι δακτύλιος μονοσήμαντης ανάλυσης.

Στην θεωρία αριθμών επεκτείνουμε την έννοια του ιδεώδους, ως εξής :

Ορισμός 1.3

Έστω R ακέραια περιοχή και K το σώμα πηλίκων της R. Το R-module $M \subseteq K$ θα λέγεται κλασματικό ιδεώδες του R αν και μόνο αν υπάρχει $x \in R$,$x \neq 0$ με $xM \subseteq R$.

Αν $x \in K$ το xR θα λέγεται κύριο κλασματικό ιδεώδες του R.

Τα συνηθισμένα ιδεώδη του R, που είναι κλασματικά για x=1 θα λέγονται ακέραια. Ο δακτύλιος των ακεραίων αλγεβρικών αριθμών R_K ενός αλγεβρικού σώματος αριθμών K είναι δακτύλιος του Dedekind (δες, [A2], Θεώρ. 2.8, σελ. 51). Μία από τις ποίο σημαντικές ιδιότητες που έχουν οι δακτύλιοι αυτοί είναι το μονοσήμαντο της ανάλυσης των ιδεωδών τους σε γινόμενο πρώτων ιδεωδών.

Στα επόμενα θα κρατήσουμε σταθερό τον παρακάτω συμβολισμό K, L, M θα είναι αλγεβρικά σώματα αριθμών με $K \subset L \subset M$. Με $R \subset S \subset T$ θα συμβολίζουμε τους αντίστοιχους δακτυλίους του Dedekind των ακεραίων αλγεβρικών αριθμών των K, L, M. Με P τα πρώτα ιδεώδη του R, Q τα πρώτα ιδεώδη του S, U τα πρώτα ιδεώδη του T. Αν λοιπόν P είναι ένα πρώτο ιδεώδες του R το PS είναι ιδεώδες του S όχι κατ΄ ανάγκην πρώτο και επειδή ο S είναι δακτύλιος του Dedekind, έχουμε

$PS=Q_1^{e_1} \ldots Q_r^{e_r}$ όπου Q_i είναι πρώτα ιδεώδη του S.

Το ερώτημα που τίθεται είναι ποια ιδεώδη υπεισέρχονται στην ανάλυση του PS και με ποιους εκθέτες.

Πρόταση 1.4

Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες :

(1)Q_i/PS δηλαδή υπάρχει ακέραιο ιδεώδες Q_i' του S με $PS=Q_iQ_i'$

(2)$Q_i \supseteq PS$

(3)$Q_i \supseteq P$

(4)$Q_i \cap R=P$

(5)$Q_i \cap K=P$.

Απόδειξη

Δές, [A2], Πρότ. 1.1, σελίδα 116.

Ορισμός 1.5

Αν ισχύει μια από τις παραπάνω σχέσεις (και συνεπώς και οι πέντε) τότε θα λέμε

(1) το Q_i βρίσκεται πάνω από το P

(2) το P βρίσκεται κάτω από το Q_i.

Θεώρημα 1.6

Έστω P ένα πρώτο ιδεώδες του R και $PS=Q_1^{e_1}\dots Q_r^{e_r}$ η ανάλυση του PS σε γινόμενο πρώτων ιδεωδών του S. Τα πρώτα ιδεώδη $Q_1,\dots, Q_r$ και μόνο αυτά βρίσκονται πάνω από το P (στην επέκταση L/K).

Απόδειξη

Έστω Q ένα πρώτο ιδεώδες του S πάνω από το P, τότε $Q\supseteq PS= PS=Q_1^{e_1}\dots Q_r^{e_r}$ άρα υπάρχει $i\in \{1,2,\dots,r\}$ όπου το Q διαιρεί το Q_i οπότε $Q_i\subseteq Q$ και αφού Q_i μέγιστο, έχουμε ότι $Q= Q_i$ και $Q \supseteq \prod_{i=1}^{r} Q_i^{e_i}=PS\supseteq P$.

Ορισμός 1.7

Ο εκθέτης e:= e(Q/P) με τον οποίο εμφανίζεται το Q στην ανάλυση του PS σε γινόμενο πρώτων παραγόντων λέγεται δείκτης διακλάδωσης του Q υπέρ το P.

Θα λέμε ότι το Q διακλαδίζεται υπέρ του P αν και μόνο αν e(Q/P)>1.

Θα λέμε ότι το P διακλαδίζεται υπέρ του L αν και μόνο αν υπάρχει Q πρώτο ιδεώδες του S με e(Q/P)>1.

Έστω τώρα ότι το Q βρίσκεται πάνω από το P, θεωρούμε την συνάρτηση :

$$i : R/P\to S/Q, \text{ με } r+P\to r+Q$$

η i είναι προφανώς μονομορφισμός σωμάτων. Ταυτίζουμε λοιπόν τα σώματα R/P και i(R/P)=(R+Q/Q), δηλαδή θεωρούμε το R/P σαν υπόσωμα του S/Q.

Ορισμός 1.8

Έστω ότι το Q βρίσκεται πάνω από το P. Τότε το f=f(Q/P)=[S/Q:R/P] θα λέγεται βαθμός αδράνειας του Q υπέρ P.

Θεώρημα 1.9

Έστω ότι [L:K]=n . Τότε ισχύει ότι $n=e_1f_1+\dots+e_rf_r=\sum_{Q\supseteq P} e(Q/P)f(Q/P)$, όπου $e_i=e(Q_i/P)$, $f_i=f(Q_i/P)$.

Απόδειξη

Δές, [A2], Θεώρημα 1.7, σελίδα.119.

Πόρισμα 1.10

Αν η επέκταση L/K είναι Galois τότε για κάθε πρώτο ιδεώδες P του R έχουμε την ανάλυση

$PS=(Q_1Q_2\dots Q_r)^e$, όπου $e=e_1=e_2=\dots=e_r$, $f=f_1=\dots=f_r$ και $n=efr$.

Απόδειξη

Δες, [A2], Πόρισμα 1.9, σελίδα. 122.

Θεώρημα 1.11

Έστω L=K(θ), θ∈ S. Αν το πρώτο ιδεώδες P του R δεν διαιρεί την διακρίνουσα $\Delta_{L/K}(\theta)$ (δες, σελ.19) τότε το P δεν διακλαδίζεται στο σώμα L. Συνεπώς υπάρχουν το πολύ πεπερασμένου πλήθους πρώτα ιδεώδη του R τα οποία διακλαδίζονται στο σώμα L.

Απόδειξη

Δες, [A2], Θεώρημα 1.18, σελίδα 136.

Διακρίνουσα σώματος και βάση ακεραιότητας

Έστω K αλγεβρικό σώμα αριθμών, K=**Q**(θ) με [K:**Q**]=n και $\omega_1,\omega_2,\ldots,\omega_n$ μια βάση της επέκτασης K/**Q**.

Έστω $\alpha_i=\sum_{j=1}^{n} \alpha_{ij}\omega_j$, j=1,2,…,n, n-στοιχεία του σώματος K, όπου $\alpha_{ij}\in$ **Q** για κάθε i=1,2,…,n, j=1,2,...,n.

Πρόταση 1.12

Ισχύει $\Delta_K(\alpha_1,\ldots,\alpha_n)=(\det([\alpha_{ij}])^2\Delta(\omega_1,\ldots,\omega_n)$.

Απόδειξη

Δες, [A2], Πρόταση 4.1, σελίδα 87.

Ορισμός 1.13

Κάθε Z-βάση του R λέγεται βάση ακεραιότητας του K υπέρ του Q.

Αν $\{\omega_1,\ldots,\omega_n\}$ μια βάση ακεραιότητας και $\Delta_K(\{\omega_1',\ldots,\omega_n'\})$ μια άλλη βάση τότε από την πρόταση 1.12 συμπεραίνουμε ότι η $\Delta_K(\{\omega_1,\ldots,\omega_n\})$ διαιρεί την $\Delta(\{\omega_1',\ldots,\omega_n'\})$ και $\Delta_K(\{\omega_1',\ldots,\omega_n'\})$ διαιρεί την $\Delta_K(\{\omega_1,\ldots,\omega_n\})$

Από τα παραπάνω συμπεραίνουμε ότι η διακρίνουσα μιας βάσης ακεραιότητας δεν εξαρτάται από την εκλογή της βάσης και ως εκ τούτου :

Ορισμός 1.14

Έστω K ένα αλγεβρικό σώμα αριθμών και $\omega_1,\ldots,\omega_n$ μια βάση ακεραιότητας της K/Q. Η διακρίνουσα $\Delta_K=\Delta_{K/Q}=\Delta_{K/Q}(\omega_1,\ldots,\omega_n)$ θα λέγεται διακρίνουσα του σώματος K.

Διακρίνουσα μιας n-άδας στοιχείων

Έστω τώρα L/K μια πεπερασμένη και διαχωρίσιμη επέκταση. Γνωρίζουμε ότι υπάρχουν ακριβώς n=[L:K] K-εμφυτεύσεις του L σε κάποια κανονική θήκη του K, έστω N, τέτοια ώστε $L \subset N$. Έστω $\sigma_1,\ldots,\sigma_n$ αυτές και έστω $(\alpha_1,\ldots,\alpha_n) \in L^n$ μια n-άδα του L.

Ορισμός 1.15
Ο αριθμός $\Delta_{L/K}(\alpha_1,\ldots,\alpha_n)=(\det(\sigma_i(\alpha_j))_{ij})^2$ θα λέγεται η διακρίνουσα της n-άδας $(\alpha_1,\ldots,\alpha_n)$.

Θεώρημα 1.16
Αν η L/K είναι επέκταση αλγεβρικών σωμάτων αριθμών με S και R όπως πάντα και P πρώτο ιδεώδες του R, τότε ισχύει η ισοδυναμία :
το P διακλαδίζεται στο L αν και μόνο αν το P διαιρεί τη διακρίνουσα.
Απόδειξη
Δες, [A2], Θεώρημα 5.2, σελίδα 193.

Το σύνολο όλων των κλασματικών ιδεωδών ενός αλγεβρικού σώματος αριθμών, αποτελεί άπειρη αβελιανή ομάδα την οποία θα συμβολίσουμε με I_K. Το σύνολο των κυρίων κλασματικών ιδεωδών του K αποτελεί υποομάδα της I_K την οποία θα συμβολίζουμε με H_K.

Ορισμός 1.17
Η ομάδα πηλίκων I_K/H_K θα λέγεται ομάδα κλάσεων ιδεωδών (class group) του σώματος K και θα συμβολίζεται με Cl_K.

Θεώρημα 1.18
Η τάξη της ομάδας κλάσεων ιδεωδών του K είναι πεπερασμένη
Απόδειξη
Δες, [A2], Θεώρημα 4.2.6, σελίδα 108.

Ορισμός 1.19
Η τάξη της ομάδας κλάσεων ιδεωδών αλγεβρικού σώματος αριθμών K λέγεται αριθμός κλάσεων ιδεωδών του σώματος K και θα συμβολίζεται με h_K.

Ισχύει το εξής :
Θεώρημα 1.20
Ο R_K είναι δακτύλιος ανάλυσης ακριβώς τότε όταν $h_K=1$.

Απόδειξη
Δες, [A2], Πρόταση 2.1, σελίδα 105.

Θεώρημα 1.21 (Minkowski)
Αν το K είναι αλγεβρικό σώμα αριθμών, $K \neq Q$ τότε η $\Delta(K/Q) \neq 1$.
Απόδειξη
Δες, [CF], σελίδα 357.

Αυτό σημαίνει ότι τουλάχιστον ένας πρώτος του **Q** διακλαδίζεται στο K.

Τέλος αναφέρουμε το ακόλουθο :
Θεώρημα 1.22 (Μονάδων του Dirichlet)
Αν K αλγεβρικό σώμα αριθμών και E(K) η ομάδα των μονάδων (εννοείται η ομάδα των μονάδων του δακτυλίου των ακεραίων αλγεβρικών αριθμών) είναι ευθύ γινόμενο μιας πεπερασμένης κυκλικής ομάδας και μίας ελεύθερης αβελιανής με $r=r_1+r_2-1$ γεννήτορες :

$$E(K)=W_K \times Z^r.$$

Απόδειξη
Δές, [CF], Th. Unit theorem, σελίδα 72.

Norm ενός στοιχείου και Norm ιδεωδών

Κάθε αλγεβρικό σώμα αριθμών K, είναι, ως γνωστό είναι μία απλή επέκταση του **Q**, δηλαδή υπάρχει ένα στοιχείο $\theta \in K$ τέτοιο ώστε $K=\mathbf{Q}(\theta)$. Αν f(x) είναι το ανάγωγο πολυώνυμο του θ περάνω του **Q**, τότε $n=[K:\mathbf{Q}]=\deg f(x)$.
Έστω $\theta_1,\theta_2,\ldots,\theta_n$ οι διακεκριμένες μεταξύ τους , ρίζες του f(x) στο **C**. Αν κάποια από αυτές τις ρίζες είναι μιγαδική τότε και οι συζυγή της είναι επίσης ρίζα του f(x). Αν λοιπόν το f(x) έχει r_1 πραγματικές ρίζες και $2r_2$ μιγαδικές ρίζες τότε

$$r_1+2r_2=n.$$

Το σώμα K επιδέχεται n εμφυτεύσεις στο σώμα C. Πρόκειται για n, **Q**-μονομορφισμούς

$$\sigma_i : K=\mathbf{Q}(\theta) \to \mathbf{Q}(\theta_i) \subseteq \mathbf{C}, \text{ όπου } \theta \to \theta_i.$$

Έστω K, L αλγεβρικά σώματα αριθμών $K \subset L$, θ ένα πρωταρχικό στοιχείο της επέκτασης L/K δηλαδή $L=K(\theta)$, $B=\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ βάση της επέκτασης.

Έστω $a \in L$ τότε υπάρχουν $\alpha_{ij} \in K$ τέτοια ώστε $a\theta^i = \sum_{j=0}^{n-1} \alpha_{ij}\theta^j$.

Συμβολίζουμε τον πίνακα $A(a)=(\alpha_{ij}) \in M_{n\times n}(K)$ και θα τον ονομάζουμε <u>πίνακα αναπαράστασης του a</u>.

<u>Ορισμός 1.23</u>
<u>Norm</u> του a ως προς την επέκταση L/K ονομάζουμε τον αριθμό $N_{L/K}(a)=detA(a)$.

Έστω $K=\mathbf{Q}(\theta)$ ένα αλγεβρικό σώμα αριθμών, R_K ο δακτύλιος του Dedekind των ακεραίων αλγεβρικών αριθμών αυτού. Για κάθε ακέραιο ιδεώδες A του R ο δακτύλιος R/A έχει πεπερασμένο πλήθος στοιχείων και αυτών τον αριθμό τον λέμε <u>norm του ιδεώδους</u> A,

$$N_K(A)=\#(R/A).$$

<u>2.Εκτιμήσεις (valuations) αλγεβρικών σωμάτων αριθμών</u>

Είναι γνωστή η μέθοδος πλήρωσης του σώματος των ρητών αριθμών **Q** ως προς την συνήθη μετρική μέσω ακολουθιών Cauchy και της κατασκευής του σώματος των πραγματικών αριθμών **R**.
Η συνήθης μετρική ορίζεται μέσω της έννοιας της απόλυτης τιμής στο **Q**.
Οι βασικές ιδιότητες της απόλυτης τιμής είναι

(i) $|x| \geq 0$, $|x|=0 \Leftrightarrow x=0$
(ii) $|x||y|=|xy|$
(iii) $|x+y| \leq |x|+|y|$ για όλα τα $x, y \in \mathbf{Q}$.

Το ερώτημα είναι αν υπάρχουν και άλλες συναρτήσεις με αυτές τις ιδιότητες που θα μπορούσαν να οριστούν στο **Q**, μέσω των οποίων θα μπορούσαμε να κατασκευάσουμε την πλήρωση του **Q**. Η απάντηση στο παραπάνω ερώτημα είναι θετική. Υπάρχουν μάλιστα συναρτήσεις οι οποίες, με κάποια έννοια, είναι πολύ καλύτερες από την απόλυτη τιμή.

<u>Ορισμός 2.1</u>

Μια εκτίμηση (valuation) ενός σώματος K είναι εξ ορισμού μια συνάρτηση

$$\upsilon : K \to R$$

τέτοια ώστε για όλα τα $x,y \in K$ να ισχύουν :

(i) $\upsilon(x) \geq 0$, $\upsilon(x)=0 \Leftrightarrow x=0$

(ii) $\upsilon(xy)=\upsilon(x)\upsilon(y)$

(iii) $\upsilon(x+y) \leq \upsilon(x)+\upsilon(y)$.

Αν αντί της (iii) ισχύει η ισχυρότερη ανισότητα,

$\upsilon(x+y) \leq \max\{\upsilon(x),\upsilon(y)\}$ **για όλα τα** $x,y \in K$

τότε η εκτίμηση θα λέγεται <u>μη αρχιμήδεια</u> αλλιώς θα λέγεται <u>αρχιμήδεια.</u>

Επομένως, η απόλυτη τιμή είναι μια αρχιμήδεια εκτίμηση του **Q**.

Σε κάθε σώμα K μπορούμε να ορίσουμε μια εκτίμηση

$\upsilon_0 : K \to R$, όπου $\upsilon_0(x)=0$ αν $x=0$ και 1 αν $x \in K^*$.

Η εκτίμηση αυτή θα λέγεται **τετριμμένη εκτίμηση**.

Έστω τώρα κάποιος p πρώτος αριθμός, τον οποίο κρατούμε σταθερό. Σύμφωνα με το θεμελιώδες θεώρημα της αριθμητικής κάθε ρητός $\alpha \in \mathbf{Q}$ $\alpha \neq 0$ γράφεται μονοσήμαντα στη μορφή $\alpha=p^a(b/c)$, όπου a, b, $c \in \mathbf{Z}$ και ο p δεν διαιρεί το bc. Ορίζουμε $\upsilon_p(\alpha)=p^{-a}$ και $\upsilon_p(0)=0$.

Εύκολα αποδεικνύεται ότι η υ_p είναι μια μη αρχιμήδεια εκτίμηση του **Q** την οποία ονομάζουμε <u>p-αδική εκτίμηση</u>.

Η πλήρωση του **Q** ως προς την p-αδική εκτίμηση υ_p μας δίνει το σώμα των **p-αδικών αριθμών $\mathbf{Q_p}$** με ενδιαφέρουσες αριθμητικές ιδιότητες. Επομένως, για κάθε πρώτο αριθμό p έχουμε και μια μη αρχιμήδεια εκτίμηση του **Q**, υ_p. Το ερώτημα αν υπάρχουν και άλλες έχει, κατ΄ ουσία, αρνητική απάντηση.

Ορίζεται μια σχέση ισοδυναμίας ανάμεσα στις εκτιμήσεις του **Q** και αποδεικνύεται το (δές, [A3], σελ31).

<u>Θεώρημα 2.2</u>

Κάθε εκτίμηση του Q είναι ισοδύναμη προς την τετριμμένη εκτίμηση ή προς μια p-αδική εκτίμηση ,για κάποιο πρώτο p, ή προς την απόλυτη τιμή. Οι εκτιμήσεις αυτές, τετριμμένη, απόλυτη τιμή καθώς και οι p-αδικές εκτιμήσεις είναι μεταξύ τους ανά δύο μη ισοδύναμες.

Έστω τώρα K ένα αλγεβρικό σώμα αριθμών και $x \in K-\{0\}$. Αν R είναι ο δακτύλιος των ακεραίων αλγεβρικών του K τότε το xR είναι το κύριο κλασματικό ιδεώδες του K. Επειδή ο R είναι δακτύλιος του Dedekind το xR αναλύεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών

$$xR=P_1^{a_1} \ldots P_r^{a_r}$$

Για κάθε πρώτο ιδεώδες P του K με $w_P(x)$ θα συμβολίζουμε τον εκθέτη του P στην ανάλυση του ιδεώδους xR σε γινόμενο πρώτων ιδεωδών. Η απεικόνιση

$\upsilon_P : K \to R$, όπου $x \to N_{K/Q}(P)^{-w(x)}$

είναι μια μη αρχιμήδεια εκτίμηση του K η οποία θα λέγεται P-αδική εκτίμηση του K.

Εντελώς ανάλογα αποδεικνύεται ότι κάθε διάφορη της τετριμμένης μη αρχιμήδεια εκτίμηση του K είναι ισοδύναμη προς μια p-αδική εκτίμηση υ_p για κάποιο πρώτο ιδεώδες P του K. Επίσης για διαφορετικά πρώτα ιδεώδη του K προκύπτουν μη ισοδύναμες μεταξύ τους εκτιμήσεις.
Η πλήρωση του σώματος K ως προς την εκτίμηση υ_P μας δίνει τα λεγόμενα P-αδικά σώματα K_P.
Μια P-αδική εκτίμηση όταν περιοριστεί στο **Q** μας δίνει μη-αρχιμήδεια εκτίμηση του **Q** άρα, κατ΄ ανάγκη, ισοδύναμη προς μια p-αδική εκτίμηση όπου $p\mathbf{Z}=P \cap \mathbf{Z}$. Επομένως οι υ_P αποτελούν επεκτάσεις των εκτιμήσεων υ_p του **Q**. Το ερώτημα που τίθεται εδώ είναι σε πόσες μη ισοδύναμες μεταξύ τους εκτιμήσεις του K επεκτείνεται η υ_p; Η απάντηση είναι όσο ακριβώς το πλήθος των πρώτων ιδεωδών του K που βρίσκονται πάνω από το pR (δες, [A3], Θεώρ. 2.3, σελ154). Αλλιώς θα μπορούσαμε να πούμε ότι είναι ίσο με το πλήθος των αναγώγων παραγόντων του $f(x)=Irr(\theta,\mathbf{Q})$ στο $(\mathbf{Z}/p\mathbf{Z})[x]$, όπου $K=\mathbf{Q}(\theta)$.
Ας περάσουμε τώρα στις αρχιμήδειες εκτιμήσεις του αλγεβρικού σώματος αριθμών K. Κάθε τέτοια εκτίμηση περιορισμένη στο **Q** θα μας δώσει αρχιμήδεια εκτίμηση του **Q** η οποία κατ΄ ανάγκη, θα είναι ισοδύναμη με την απόλυτη τιμή. Δηλαδή οι αρχιμήδειες εκτιμήσεις του K είναι επεκτάσεις της απόλυτης τιμής του **Q**.
Αν $\sigma_i : K \to \mathbf{R}$ $i=1,2,\ldots r_1$ οι πραγματικές εμφυτεύσεις του K στο **C** και σ_i, σ_i' τα ζευγάρια των συζυγών μιγαδικών εμφυτεύσεων αυτού οι συναρτήσεις

$$\upsilon_i : K \to \mathbf{R}, \text{ όπου } x \to |\sigma_i(x)|, \ i=1,2,\ldots,r_1+r_2.$$

είναι μη ισοδύναμες ανά δυο αρχιμήδειες εκτιμήσεις του σώματος K, όπου $|\sigma_i(x)|$ είναι η συνηθισμένη απόλυτη τιμή στο **R**, C αντίστοιχα. (Παρατηρούμε ότι συζυγείς μιγαδικές εμφυτεύσεις δίνουν ισοδύναμες εκτιμήσεις, διότι $|\sigma_i(x)|= |\sigma_i'(x)|$ για κάθε $x \in K$.)

Θεώρημα 2.3
Κάθε αρχιμήδεια εκτίμηση του K είναι ισοδύναμη προς μια από τις εκτιμήσεις υ_i, $i=1,2,\ldots,r_1+r_2$.

Απόδειξη
Δες, [J], Λήμμα 4.3 θεώρημα 5.1, σελ 87.

Αν τώρα θεωρήσουμε την πλήρωση του K ως προς κάποια αρχιμήδεια εκτίμηση υ_i τότε το σώμα που θα προκύψει θα είναι το **R** ή το **C** σύμφωνα με το :

Θεώρημα 2.4 (Θεώρημα Ostrowski)
Τα μόνα πλήρη σώματα ως προς μια αρχιμήδεια εκτίμηση είναι το σώμα των πραγματικών και το σώμα μιγαδικών αριθμών.
Απόδειξη
Δες, [A3], Θεώρημα 1.11, σελ147.

3. Idele

Η αμφιμονοσήμαντη αντιστοιχία που μελετήσαμε στην προηγούμενη παράγραφο μεταξύ των πρώτων ιδεωδών του K και των κλάσεων μη ισοδύναμων αρχιμήδειων εκτιμήσεων αυτού μας υποβάλλει την ιδέα να τροποποιήσουμε την ορολογία μας.
Κάθε κλάση ισοδύναμων εκτιμήσεων του K θα λέγεται ένας **πρώτος** του K. Αν η κλάση περιέχει μια αρχιμήδεια εκτίμηση θα λέγεται **άπειρος πρώτος** αλλιώς θα λέγεται **πεπερασμένος πρώτος**.
Ένας άπειρος πρώτος θα λέγεται **πραγματικός** αν η πλήρωση του K ως προς αυτόν τον πρώτο είναι το σώμα των πραγματικών **R** ενώ αν είναι το σώμα των μιγαδικών **C** θα λέγεται **μιγαδικός πρώτος**.
Αν τώρα ο p είναι ένας άπειρος πρώτος του **Q** και $P_1,P_2,\ldots,P_r$ οι διακεκριμένοι μεταξύ τους άπειροι πρώτοι του K που βρίσκονται πάνω από το p ,θα λέμε ότι ο P_i **δεν διακλαδίζεται** αν οι πληρώσεις του K ως προς P_i και του Q ως προς τον p συμπίπτουν. Δηλαδή αν είναι και οι δυο πληρώσεις συγχρόνως ίσες με το σώμα των πραγματικών ή το σώμα των μιγαδικών αριθμών.
Η αριθμητική ενός αλγεβρικού σώματος αριθμών αντανακλάται σε ιδιότητες των πληρώσεων K_P όπου P πρώτος του K. Αντί όμως να μελετούμε κάθε σώμα K_P χωριστά θα προσπαθήσουμε να ενοποιήσουμε την μελέτη τους μέσω μιας καινούργιας έννοιας, αυτής των idele. Πρόκειται για μια έννοια που έχει εισαγάγει ο Claude Chevalley. Η ονομασία προκύπτει από την συνένωση των πρώτων συλλαβών των λέξεων ideale Elemente. Η σημασία του είναι πολύ σημαντική διότι επιτρέπει κατά θαυμάσιο τρόπο το πέρασμα από την θεωρία των τοπικών P-αδικών σωμάτων K_P στα αλγεβρικά σώματα αριθμών K. Για μια αναλυτική ανάπτυξη του

θέματος παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο (δες, [N1], Teil II, σελ.195-232).
Έστω λοιπόν K ένα αλγεβρικό σώμα αριθμών. Ένα idele A του K είναι μια οικογένεια $A=(A_P)$ αριθμών όπου $A_P \in K_P^* = K_P-\{0\}$, και το P διατρέχει όλους τους πρώτους P του K και όπου τα A_P είναι μονάδες του σώματος K_P για σχεδόν όλους, εκτός από πεπερασμένο πλήθος, πρώτους P. Θα μπορέσουμε να πάρουμε την έννοια του idele μέσω του ακόλουθου

<u>Ορισμός 3.2</u>
Έστω S πεπερασμένο σύνολο πρώτων του σώματος K. Η ομάδα

$$\mathbf{J_K^S=\prod_{P\in S} K_P^* \times \prod_{P\notin S} U_P \subseteq \prod_P K_P}$$

λέγεται <u>ομάδα των S-idele</u>.

Με U_P συμβολίζουμε την ομάδα των μονάδων του σώματος K_P όταν ο πρώτος P είναι πεπερασμένος και την ομάδα K_P^* όταν ο P είναι άπειρος.
Η ένωση

$$J_K=\bigcup_S J_K^S \subseteq \prod_P K_P$$

όπου το S διατρέχει όλα τα δυνατά πεπερασμένα σύνολα πρώτων του K λέγεται **ομάδα των idele του K**.
Αν $A=(A_P)\in J_K$, $A_P\in K_P^*$ τότε οι αριθμοί A_P λέγονται **συνιστώσες του idele**. Μια συνιστώσα A_P λέγεται **βασική** όταν το A_P δεν είναι μονάδα του K_P.
Ένα idele έχει επομένως το πολύ πεπερασμένου πλήθους βασικές συνιστώσες, ένα S-idele έχει βασικές συνιστώσες το πολύ για τους πρώτους P που ανήκουν στο σύνολο S. Ο λόγος για τον οποίο απαιτούμε σχεδόν όλες οι συνιστώσες ενός idele να μην είναι βασικές, είναι ότι κατ΄ αυτό τον τρόπο επιτυγχάνουμε να εμφυτεύσουμε την πολλαπλασιαστική ομάδα K^* του σώματος K κατά κανονικό τρόπο μέσα στην ομάδα των idele.
Πράγματι, αν $x\in K^*$ με (x) θα συμβολίζουμε εκείνο το idele της ομάδας J_K για το οποίο όλες οι συνιστώσες είναι ίσες με x δηλαδή $(x)_P=x\in K_P^*$.
Αρκεί λοιπόν να παρατηρήσει κανείς ότι το x είναι για σχεδόν όλους τους πρώτους P του K, μια μονάδα του K_P. Κατ΄ αυτό τον τρόπο εμφυτεύουμε την ομάδα K^* στην ομάδα των idele J_K. Τα idele της K^* λέγονται **κύρια idele**. Αν τώρα S είναι ένα πεπερασμένο σύνολο πρώτων του K με K^S θα συμβολίζουμε την ομάδα $K^S=K^*\cap J_K^S \subseteq J_K^S$ των **S-κυρίων idele**. Τα στοιχεία του K^S λέγονται και <u>S-μονάδες</u> του K διότι είναι μονάδες για κάθε πρώτο P του K, $P\notin S$. Αν τώρα πάρουμε ειδικά $S=S_\infty$ το σύνολο όλων των άπειρων πρώτων του K τότε η ομάδα K^{S_∞} είναι η ομάδα των μονάδων του K.

Ορισμός 3.3

Η ομάδα πηλίκων $C_K=J_K/K^*$ λέγεται ομάδα κλάσεων των idele (idele class group) του σώματος K.

Εντελώς φυσιολογικά τώρα τίθεται το ερώτημα: Ποια σχέση έχουν τα idele με τα ιδεώδη ;
Η σχέση αυτή δίνεται από το επόμενο θεώρημα :

Θεώρημα 3.4

Αν με S_∞ συμβολίζουμε το σύνολο όλων των άπειρων πρώτων του αλγεβρικού σώματος αριθμών K, $(J_K)^{S_\infty}$ την ομάδα των idele τα οποία έχουν συνιστώσα μονάδα σε κάθε πεπερασμένο πρώτο P του K, τότε ισχύουν :

$J_K/(J_K)^{S_\infty}=I_K$ και $J_K/((J_K)^{S_\infty}K^*)=I_K/H_K=Cl_K$

Απόδειξη

Δές, [N1], Θεώρημα 23, σελίδα 197.

Η ομάδα κλάσεων των idele C_K δεν είναι πεπερασμένη σε αντίθεση με την ομάδα των κλάσεων ιδεωδών Cl_K.
Αν L/K είναι μια επέκταση αλγεβρικών σωμάτων μπορούμε, κατά φυσιολογικό τρόπο να εμφυτεύσουμε τα idele του K στα idele του L και να θεωρήσουμε την ομάδα των idele του K, J_K σαν υποομάδα των idele του L J_L, $J_K \to J_L$.
Αν τώρα η επέκταση L/K είναι επέκταση Galoisμε ομάδα του Galois, G:=Gal(L/K),τότε ισχύει :

$J_L{}^G=J_K$

(δές,)

Ένα σημαντικό αποτέλεσμα το οποίο θα χρησιμοποιήσουμε στα επόμενα είναι το

Θεώρημα 3.5

Ισχύει :

$H^1(G,U_K)=1$

Απόδειξη

Δές,

Παρατήρηση 3.5

Είναι γνωστό ότι είναι δυνατό ένα ιδεώδες αλγεβρικού σώματος αριθμών K να μην είναι κύριο στο K ενώ να γίνεται κύριο σε κάποια επέκταση του K, π.χ στο σώμα του Hilbert αυτού. Για τα idele έχουμε εντελώς διαφορετική συμπεριφορά. Συγκεκριμένα ισχύει

$$\mathbf{L^* \cap J_K=K^*}$$

Απόδειξη
Δες, [N1], Satz 2.6, σελ 202.

ΚΕΦΑΛΑΙΟ 3

Στο κεφάλαιο αυτό θα διατυπώσουμε και θα αποδείξουμε το θεώρημα των Golod - Shafarevich.
Υπενθυμίζουμε ότι το πρόβλημα της εμφύτευσης ενός αλγεβρικού σώματος αριθμών k είναι το πρόβλημα της ύπαρξης αλγεβρικού σώματος αριθμών K, $k \subseteq K$ με αριθμό κλάσεων ιδεωδών $h_K=1$.
Αν τώρα με K_i συμβολίσουμε το σώμα του Hilbert του K_{i-1} (i=1,2,…), $K_0:=k$ τότε η ένωση

$$k_\infty = \bigcup_{i=1}^{\infty} K_i$$

μας δίνει μια αλγεβρική επέκταση του k, k_∞/k η οποία όμως μπορεί να είναι άπειρη επέκταση του k.
Θα αποδείξουμε την ακόλουθη πρόταση:

Πρόταση 3.1
Αν μπορούμε να εμφυτεύσουμε το σώμα k σε κάποιο σώμα K, $k \subset K$ με $h_K=1$ τότε $k_\infty \subset K$. Οπότε η επέκταση k_∞/k είναι πεπερασμένου βαθμού.
Αντιστρόφως, αν ο βαθμός του k_∞/k είναι πεπερασμένος τότε έχουμε $h_{k_\infty}=1$ και συνεπώς το k_∞ είναι η μικρότερη λύση στο ερώτημα της εμφύτευσης.

Απόδειξη

Θα αποδείξουμε ότι $K_i \subset K$ για κάθε $i \in \mathbf{N}$ όπου K_i τα σώματα του πύργου των κλάσεων του Hilbert. Η απόδειξη θα γίνει με μαθηματική επαγωγή. Αρκεί να το αποδείξουμε για το K_1.
Η K_1/k είναι αβελιανή επέκταση Galois. Επομένως, σύμφωνα με το θεώρημα της μεταφοράς (δες, [Λ], σελ.264), η επέκταση K_1K/K είναι αβελιανή. Η επέκταση K_1/K είναι επίσης μη-διακλαδιζόμενη. Επομένως, και η επέκταση K_1K/K είναι μη-διακλαδιζόμενη (δες, [Η], πρόταση 41, σελ.

61). Συνεπώς η K_1K/K είναι αβελιανή και μη–διακλαδιζόμενη. Αν K_1 το σώμα το Hilbert του L τότε η K_1/K είναι maximal ως προς τις επεκτάσεις του K που είναι μη διακλαδιζόμενες και αβελιανές άρα $K_1 K \subset K_1$. Αλλά $h_K=1$ οπότε $[K_1:K]=1$ άρα $K= K_1$, δηλαδή $K_1 K \subset K$ άρα $K_1 \subset K$.

Αντίστροφο:

Επειδή επέκταση k_∞/k είναι πεπερασμένη έχουμε οτι υπάρχει $i \in \mathbf{N}$ με $k_\infty \subset K_i$. Αλλά $K_i \subset k_\infty$ οπότε $K_i = k_\infty$. Άρα $h_{k_\infty} = h_{Ki} = [K_{1+i} : K_i]$.

Αλλά $K_{1+i} \subset k_\infty \subset K_i$ και $K_i \subset K_{1+i}$. Άρα $K_i = K_{1+I}$, οπότε $h_{K_\infty} = h_K = [K_{1+i} : K_i] = 1$.

Άρα $h_{k_\infty} = 1$.

Επομένως, αρκεί να μελετήσουμε το πρόβλημα του πύργου των κλάσεων σωμάτων.

Στα επόμενα θα προσπαθήσουμε να περιοριστούμε σε αλγεβρικές επεκτάσεις που έχουν σαν ομάδα Galois μια p-ομάδα. Ο λόγος είναι ότι μπορούμε να δουλέψουμε πολύ καλύτερα με αυτές από ότι με τυχαίες επιλύσιμες ομάδες.

Ορισμός 3.2

Έστω $p \in P$ πρώτος. Η επέκταση L/k λέγεται p-επέκταση αν

(i) η K/k είναι επέκταση Galois

και (ii) η ομάδα Gal(K/k) είναι p-ομάδα.

Σημείωση

Αν η K/k δεν είναι Galois δεν λέγεται p-επέκταση ακόμη και αν ο βαθμός της επέκτασης είναι δύναμη του p.

Έστω τώρα $K_1^{(p)}$ η μέγιστη p-επέκταση του k που περιέχεται στο K_1. Το σώμα $K_1^{(p)}$ ονομάζεται p-σώμα κλάσεων του Hilbert του k.

Έστω $K_2^{(p)}$ το p-σώμα κλάσεων του Hilbert του $K_1^{(p)}$.

Οπότε κατασκευάζουμε πύργο

$$k \subset K_1^{(p)} \subset K_2^{(p)} \subset \dots$$

ο οποίος ονομάζεται πύργος των p-κλάσεων σωμάτων του Hilbert του K.

Θέτουμε

$$k_\infty^{(p)} = \bigcup_{i=1}^{\infty} K_i^{(p)} .$$

Ισχύει $K_i^{(p)} \subset K_i$ οπότε η $K_i^{(p)}$ είναι η μέγιστη p-επέκταση του k που περιέχεται στο K_i. Συνεπώς $k_\infty^{(p)} \subset k_\infty$ και επομένως, αν η επέκταση $k_\infty^{(p)}$ /k είναι άπειρη τότε θα είναι άπειρη και η επέκταση k_∞ /k.
Επομένως αν πάρουμε κάποιο πρώτο αριθμό p προκύπτει το ερώτημα , κάτω από ποιες προϋποθέσεις η επέκταση $k^{(p)}$ είναι πεπερασμένου βαθμού;

Σημείωση3.3
Θα ασχοληθούμε με την $k_\infty^{(p)}$ αντί της k_∞ διότι οι p-ομάδες είναι πιο εύχρηστο «εργαλείο» από τις τυχαίες ομάδες. Εντελώς ανάλογα προς την πρόταση 3.1 αποδεικνύεται η πρόταση :

Πρόταση 3.4
Έστω p πρώτος αριθμός. Αν το πρόβλημα της εμφύτευσης $k \subset K$ όπου ο p δεν διαιρεί τον αριθμό κλάσεων h_K έχει λύση K τότε $k_\infty^{(p)} \subset K$ και $k_\infty^{(p)}$ /K είναι πεπερασμένη.
Αντιστρόφως αν $k_\infty^{(p)}$ /K είναι πεπερασμένη, τότε ο p δεν διαιρεί τον $h_{k_\infty^{(p)}}$, οπότε η επέκταση $k_\infty^{(p)}$ είναι η μικρότερη λύση στο πρόβλημα της εμφύτευσης ως προς τον πρώτο p.

Ορισμός 3.5
Έστω G οποιαδήποτε ομάδα, με G/p θα συμβολίζουμε τη μέγιστη αβελιανή ομάδα πηλίκων της G με εκθέτη p, θεωρούμενη ως διανυσματικός χώρος πάνω από το σώμα F_p με p στοιχεία.
Η διάσταση αυτού του διανυσματικού χώρου είναι $d^{(p)}$ G = dim G/p και ονομάζεται p-rang της G.

Παρατήρηση 3.6
Αν η G είναι πεπερασμένη αβελιανή ομάδα τότε ο $d^{(p)}$ G είναι ο αριθμός των παραγόντων τάξεως δύναμης του p που εμφανίζονται στην ανάλυση της G σε κυκλικές συνιστώσες.

ΘΕΩΡΗΜΑ 3.7 (Golod – Shafarevich)
Υπάρχει συνάρτηση γ(n) η οποία εξαρτάται από το n τέτοια ώστε $d^{(p)} Cl_k < \gamma(n)$ για κάθε αλγεβρικό σώμα αριθμών k με βαθμό n υπέρ το Q του οποίου ο πύργος p κλάσεων είναι πεπερασμένος.

Σημείωση 3.8

Στην απόδειξη του θεώρηματος θα δούμε οτι

$$d^{(p)}Cl_k<2+2\sqrt{r_k+\delta_k^{(p)}}$$

όπου r_k : ο αριθμός των άπειρων πρώτων του k

$\delta_k^{(p)}$ =1 ή 0 ανάλογα με το αν οι p-ρίζες της μονάδας ανήκουν στο k ή όχι.

Επειδή $r_k \le n$ και $\delta_k^{(p)} \le 1$ μπορούμε να πάρουμε

$$\gamma(n)=2+2\sqrt{n+1}.$$

Προκειμένου να αποδείξουμε το επόμενο θεώρημα, εισάγουμε τον ακόλουθο συμβολισμό.

Ορισμός 3.9

Έστω $q \in Z$ πρώτος και έστω D οποιοσδήποτε πρώτος του k που είναι επέκταση του q στο k με δείκτη διακλάδωσης e(D).

Θέτουμε $e_k(q)=M.K.Δ.\{e(D)\}=M.K.Δ(e_1,\ldots,e_s)$ όπου το D διατρέχει όλες τις επεκτάσεις του q στο k.

Θα λέμε ότι ο q διακλαδίζεται πλήρως στο k αν $e_k(q)>1$.

Θέτουμε $t_k^{(p)}$ το πλήθος των πλήρων διακλαδιζόμενων q τέτοια ώστε το p διαιρεί το $e_k(q)$.

ΘΕΩΡΗΜΑ 3.10 (Brumer)

Υπάρχει συνάρτηση c(n), εξαρτούμενη μόνο από το n, τέτοια ώστε

$$d^{(p)}Cl_k \ge t_k^{(p)}-c(n)$$

για κάθε αλγεβρικό σώμα αριθμών k βαθμού n, υπέρ το Q.

Σημείωση 3.11

Θα δούμε οτι μπορούμε να αποδείξουμε ότι

$$d^{(p)}Cl_k \ge t_k^{(p)}-r_k n$$

και, επειδή $r_k \le n$, μπορούμε να πάρουμε

$$c(n)=n^2.$$

Σημείωση 3.12

Θα αποδείξουμε το παραπάνω θεώρημα μόνο στην περίπτωση που η k/Q είναι επέκταση Galois. Θα δούμε οτι υπάρχει συνάρτηση c΄(n) τέτοια ώστε για κάθε επέκταση Galois βαθμού n ισχύει

$$d^{(p)}Cl_k \ge t_k^{(p)}- c΄(n).$$

Συγκεκριμένα, για επεκτάσεις Galois, θα αποδείξουμε οτι

$$d^{(p)}\,Cl_k \geq t_k^{(p)}-((r_k-1)/(p-1)+w_p(n)\delta_k^{(p)})$$

όπου $w_p(n)$ είναι ο εκθέτης του p που εμφανίζεται στην ανάλυση του n σε γινόμενο πρώτων παραγόντων. Επειδή $w_p(n)\leq n-1$, μπορούμε να πάρουμε

$$c'(n)=(n-1)+(n-1)=2(n-1).$$

Συνδυάζοντας τώρα τα θεωρήματα των Golod-Shafarevich και Brumer έχουμε το

Πόρισμα 3.13

Αν το k είναι αλγεβρικό σώμα αριθμών με βαθμό n=[k:Q] και αν

$$t_k^{(p)} \geq \gamma(n)+c(n)$$

τότε ο p-πύργος κλάσεων σωμάτων του k είναι άπειρος.

Ειδικά για κάθε n>1 και για κάθε p πρώτο ο οποίος δεν διαιρεί τον n υπάρχουν άπειρα στο πλήθος αλγεβρικά σώματα k βαθμού n με άπειρο p–πύργο κλάσεων σωμάτων.

Για παράδειγμα $k=\mathbf{Q}(\sqrt[n]{q_1 \ldots q_N})$ με $N\geq\gamma(n)+c(n)$ όπου $q_i>0$ πρώτος του **Q,** για κάθε i=1,2,…,N.

Αριθμητικό παράδειγμα

Θεωρούμε την περίπτωση όπου n=p=2 τότε έχουμε $\delta_\kappa^{(2)}=1$,$w_2(2)=1$. Επειδή $t_k^{(2)}$ είναι ο αριθμός των πεπερασμένων πρώτων του **Q** οι οποίοι διακλαδίζονται στο k προκύπτει ότι: Ένα τετραγωνικό σώμα K έχει έναν άπειρο 2-πύργο κλάσεων σωμάτων αν ο αριθμός των πρώτων του **Q** οι οποίοι διακλαδίζονται στο K είναι μεγαλύτερος ίσος του $2+2\sqrt{r_k+1+r_k}$.

Αν το k είναι φανταστικό έχουμε $r_k=1$ οπότε $2+2\sqrt{2+1}<6$, άρα ένα φανταστικό σώμα με τουλάχιστον 6 διακλαδιζόμενους πρώτους έχει έναν άπειρο 2-πύργο κλάσεων σωμάτων. Ένα μικρό αριθμητικό παράδειγμα είναι το εξής:

$$k = \mathbf{Q}(\sqrt{(-2.3.5.7.11.13.19}\,)=\mathbf{Q}\,(\sqrt{-30030}\,).$$

Αν το k είναι πραγματικό έχουμε $r_k=2$, οπότε $2+2\sqrt{3+2}$ <8, άρα βλέπουμε ότι στην περίπτωση που το k είναι πραγματικό πρέπει να έχουμε τουλάχιστον 8 πεπερασμένους διακλαδιζόμενους πρώτους για να προκύψει ένας άπειρος 2-πύργος κλάσεων σωμάτων. Για παράδειγμα

$$k = \mathbf{Q}\,(\sqrt{2.3.5.7.11.13.17.19}\,)=\mathbf{Q}\,(\sqrt{9699690}\,).$$

Απόδειξη του θεωρήματος των Golod-Shafarevich

Εισάγουμε κατ' αρχήν τους παρακάτω συμβολισμούς

C_k: θα συμβολίζουμε την κλάση των idele του k

U_k: θα συμβολίζουμε την ομάδα των μονάδων των idele του k

$E_k=U_k \cap k$: θα συμβολίζουμε την ομάδα των μονάδων του k

W_k: θα συμβολίζουμε την ομάδα των ριζών της μονάδας στο k

$K= k_\infty^{(p)}$

G=Gal(K/k).

Υπό την προϋπόθεση ότι η επέκταση K/k είναι πεπερασμένου βαθμού θα αποδείξουμε την ανισότητα

$$d^{(p)}Cl_k<2+2\sqrt{r_k+\delta_k^{(p)}}$$

Η απόδειξη θα γίνει σε δυο βήματα.

Στο πρώτο θα ανάγουμε το θεώρημα σε ένα αποτέλεσμα της Θεωρίας Ομάδων. Στο δεύτερο θα αποδείξουμε το αποτέλεσμα αυτό.

Βήμα 1:

Υπενθυμίζουμε το θεώρημα των μονάδων του Dirichlet, η ομάδα των μονάδων E_k, αλγεβρικού σώματος αριθμών k, είναι το ευθύ άθροισμα της πεπερασμένης κυκλικής ομάδας W_k και μιας ελεύθερης αβελιανής ομάδας με r_k-1 γεννήτορες δηλαδή $E_k=W_k x \mathbf{Z}^{r_\kappa}$.

όπου $r=rang E_k=r_k-1$ με $r_k=r_1+r_2$. Επομένως $d^{(p)}E_k=(r_k-1)+d^{(p)}W_k=(r_k-1)+\delta_k^{(p)}$.

Άρα $r_k+ \delta_k^{(p)}= d^{(p)}E_k+1$ οπότε $d^{(p)}E_k= d^{(p)}W_k+ d^{(p)}(\mathbf{Z}^{(r_\kappa-1)})$.

Επομένως αρκεί να αποδείξουμε οτι

$$d^{(p)}Cl_k<2+2\sqrt{d^{(p)}E_k+1},$$

δηλαδή ότι

$$½(\, d^{(p)}Cl_k-2)<\sqrt{d^{(p)}E_k+1}.$$

Η τελευταία όμως, ανισότητα είναι ισοδύναμη με την

$$¼\,(d^{(p)}Cl_k)^2- d^{(p)}Cl_k< d^{(p)}E_k.$$

Ισχυρισμός:

$$d^{(p)}Cl_k= d^{(p)}\,G$$

Εξ΄ ορισμού του p-rank μιας ομάδας G, έχουμε

$$d^{(p)}G= d^{(p)}\,G^{ab}$$

όπου G^{ab} είναι η μέγιστη αβελιανή ομάδα πηλίκων της G.

Η ομάδα G^{ab} αντιστοιχεί, λόγω θεωρίας Galois, στο υπόσωμα του K το οποίο είναι maximal αβελιανή επέκταση ως προς το k. Επειδή $K=k_\infty^{(p)}$, έπεται ότι το σώμα που αντιστοιχεί στην ομάδα G^{ab} είναι το p-σώμα κλάσεων του Hilbert του k.

Επομένως σύμφωνα με το νόμο αντιστροφής του Artin (δες, [N], σελίδα)

$$G^{ab}=Cl_k^{(p)}$$

όπου $Cl_k^{(p)}$ η p-Sylow υποομάδα της Cl_k.
Από τον ορισμό του p-rank, προκύπτει ότι

$$d^{(p)}\, Cl_k^{(p)} = d^{(p)} Cl_k$$

Συνεπώς, $d^{(p)}\, G = d^{(p)}\, G^{ab} = d^{(p)} Cl_k^{(p)} = d^{(p)} Cl_k$.
Επομένως η σχέση

$$¼\, (d^{(p)} Cl_k)^2 - d^{(p)} Cl_k < d^{(p)} E_k$$

είναι ισοδύναμη με την

$$¼\, (d^{(p)} G)^2 - d^{(p)} G < d^{(p)} E_k$$

Κάθε ομάδα πηλίκων της E_k έχει p-rank $\leq d^{(p)} E_k$, οπότε θα ισχύει και για την ομάδα $E_k / N_{K/k}(E_K)$. Η $N_{K/k}$ είναι ως γνωστό, μία συνάρτηση του Κστο k. Ιδιαίτερα, οι μονάδες του K, απεικονίζονται σε μονάδες του k, δηλαδή $N_{K/k}(E_K) \subset E_k$.
Αλλά $E_k / N_{K/k}(E_K) = H^0(G, E_K)$.
<u>Σημείωση</u>: Επειδή η ομάδα G είναι σταθερή σε όλη την εργασία για λόγους ευκολίας θα συμβολίζουμε την συνομολογία χωρίς αναφορά στην ομάδα G.

Επομένως, αρκεί να αποδείξουμε ότι

$$¼\, (d^{(p)} Cl_k)^2 - d^{(p)} G < d^{(p)}\, H^0(E_K).$$

Η ακολουθία των G-modules

$$1 \rightarrow E_K \rightarrow U_K \rightarrow U_K / E_K \rightarrow 1$$

είναι ακριβής. Επειδή η επέκταση K/k είναι μη διακλαδιζόμενη η U_K είναι συνομολογιακά τετριμμένη ως G-module. Αυτό το βλέπουμε ως εξής:
Αναλύουμε την ομάδα των μονάδων idele στις τοπικές συνιστώσες και εφαρμόζουμε γνωστό θεώρημα για τοπικά σώματα αριθμών (δες, [N1], Prop.43, σελίδα 137).
Επομένως η ακολουθία συνομολογίας

$$\ldots \rightarrow H^{-1}(U_K) \rightarrow H^{-1}(U_K / E_K) \rightarrow H^0(E_K) \rightarrow H^0(U_K) \rightarrow \ldots.$$

είναι ακριβής.
Αλλά

$$H^{-1}(U_K) = H^0(U_K) = 1$$

Άρα, η παραπάνω ακριβής ακολουθία γράφεται

$$1 \rightarrow H^{-1}(U_K / E_K) \rightarrow H^0(E_K) \rightarrow 1 \rightarrow \ldots.$$

Οπότε

$$H^{-1}(U_K / E_K) = H^0(E_K)$$

Επομένως η προς απόδειξη ανισότητα

$$¼\, (d^{(p)} G)^2 - d^{(p)} G < d^{(p)}\, H^0(E_K)$$

γίνεται

$$¼\, (d^{(p)} G)^2 - d^{(p)} G < d^{(p)}\, H^{-1}(U_K / E_K)$$

Στη συνέχεια χρησιμοποιούμε την ακριβή ακολουθία

$$1 \rightarrow U_K / E_K \rightarrow C_K \rightarrow Cl_K \rightarrow 1$$

Επειδή K= $k_\infty^{(p)}$ είναι το maximal σώμα του πύργου των p-κλάσεων σωμάτων του Hilbert, έχουμε ότι ο p δεν διαιρεί την τάξη της Cl_K.
Η G είναι p-ομάδα και η Cl_K είναι G-module τέτοιο ώστε ο p δεν διαιρεί τον h_k. Επομένως έχουμε ότι

$$H^q(Cl_K)=1,$$

δηλαδή η Cl_K είναι συνομολογιακά τετριμμένο G-module.
Από την προηγούμενη ακριβή ακολουθία έπεται η ακρίβεια της

$$\dots \rightarrow H^{-2}(Cl_K) \rightarrow H^{-1}(U_K/ E_K) \rightarrow H^{-1}(C_K) \rightarrow H^{-1}(Cl_K) \rightarrow \dots.$$

Αλλά

$$H^{-2}(Cl_K) =H^{-1}(Cl_K)=1.$$

Άρα η ακολουθία

$$1\rightarrow H^{-1}(U_K/ E_K) \rightarrow H^{-1}(C_K) \rightarrow 1$$

είναι ακριβής, οπότε

$$H^{-1}(U_K/ E_K)= H^{-1}(C_K),$$ (δες, [CF], Application 11.3, σελ.197)

Αλλά από το Θεώρημα του Tate έχουμε

$$H^{-1}(C_K)= H^{-3}(\mathbf{Z})$$

Αλλά

$$H^{-3}(\mathbf{Z})= H_2(\mathbf{Z})$$

και επομένως $H^{-1}(U_K/ E_K)= H^{-3}(\mathbf{Z})$.

Οπότε η προς απόδειξη ανισότητα γίνεται

$$¼ (d^{(p)}G)^2 - d^{(p)}G < d^{(p)} H_2(\mathbf{Z})$$

Βήμα 2:
Θα αποδείξουμε ότι η παραπάνω ανισότητα είναι αληθής για κάθε πεπερασμένη p-ομάδα G.
Η $\mathbf{Z}/p$ είναι κυκλική ομάδα με p στοιχεία. Επειδή οι ομάδες ομολογίας $H_i(\mathbf{Z}/p)$ μηδενίζονται όταν πολλαπλασιαστούν με p, τις θεωρούμε ως διανυσματικό χώρο πάνω από το σώμα $\mathbf{F}_p$ και συμβολίζουμε

$$d_i^{(p)}G:=\dim_{\mathbf{F}p} H_i(\mathbf{Z}/p).$$

Λήμμα 3.13
Για κάθε ομάδα G υπάρχει ένας φυσικός ισομορφισμός

$$\mathbf{H_1(Z/p)=G/p.}$$

Ιδιαίτερα

$$\mathbf{d_1^{(p)}G= d^{(p)}G.}$$

Απόδειξη
Θεωρούμε την ακριβή ακολουθία

$$0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Z} \rightarrow \mathbf{Z}/p \rightarrow 0$$

όπου η απεικόνιση p:**Z**→ **Z** είναι ο πολαπλασιασμός με p και η ψ:**Z**→**Z**/p με ψ(m)=m modp. Η ακολουθία αυτή επάγει ακριβή ακολουθία των ομάδων ομολογίας

$$\ldots\rightarrow H_i(\mathbf{Z}) \xrightarrow{p} H_i(\mathbf{Z})\rightarrow H_i(\mathbf{Z}/p) \rightarrow H_{i-1}(\mathbf{Z}) \xrightarrow{p} H_{i-1}(\mathbf{Z}) \rightarrow \ldots.$$

Γενικά γνωρίζουμε ότι

«Αν Α αβελιανή ομάδα και A_p=Ker{p:A→A} τότε το cokernel είναι A/p».

Επομένως η παραπάνω ακολουθία μας δίνει την ακόλουθη ακριβή ακολουθία

$$0 \rightarrow H_i(\mathbf{Z}) /p \rightarrow H_i(\mathbf{Z}/p) \rightarrow H_{i-1}(\mathbf{Z})_p \rightarrow 0$$

διότι φ:A→A, με φ(α)=pα οπότε Imφ=pA, Ker{αϵA:pα=0}.

Η ακολουθία

$$H_i(\mathbf{Z}) \rightarrow H_i(\mathbf{Z})\rightarrow H_i(\mathbf{Z}/p) \rightarrow H_{i-1}(\mathbf{Z}) \rightarrow H_{i-1}(\mathbf{Z}/p) \rightarrow H_i(\mathbf{Z})$$

είναι ακριβής, άρα Imφ=kerπ, Imπ=kerδ, Imδ=kerφ.

Οπότε, από το 1ο Θεώρημα Ισομορφίας, έχουμε

$$H_i(\mathbf{Z}/p)/Ker\delta=Im\delta$$

και συνεπώς

$$0 \rightarrow Ker\delta(=ker\pi) \rightarrow H_i(\mathbf{Z}/p) \rightarrow Im\delta(=ker\varphi) \rightarrow 0.$$

Στο $H_i(\mathbf{Z})$, από το 1ο Θεώρημα Ισομορφίας, έχουμε

$$0 \rightarrow ker\pi \rightarrow H_i(\mathbf{Z}) \rightarrow Im\pi(=Ker\delta) \rightarrow 0.$$

Επομένως

$$Ker\delta= Im\pi= H_i(\mathbf{Z})/ ker\pi= H_i(\mathbf{Z})/ Im\varphi= H_i(\mathbf{Z})/p$$

Οπότε έχουμε το ζητούμενο.

Για i=1 έχουμε $H_0(\mathbf{Z})=H^{-1}(\mathbf{Z})= \mathbf{Z}$, αλλά το **Z** δεν έχει p-torsion άρα $H_0(\mathbf{Z})_p$= kerφ=0

Οπότε η ακολουθία

$$0 \rightarrow H_i(\mathbf{Z})/p \rightarrow H_i(\mathbf{Z}/p) \rightarrow 0$$

είναι ακριβής, το οποίο σημαίνει οτι

$$H_i(\mathbf{Z})/p=H_i(\mathbf{Z}/p)$$

Γνωρίζουμε όμως ότι (δες, [AW], Def., σελίδα 102)

$$H_1(\mathbf{Z})= H^{-2}(\mathbf{Z})$$

και ότι $H^{-2}(\mathbf{Z})= H^1(G,\mathbf{Q}/\mathbf{Z})=G/[G,G]=G^{ab}$ (δες, Κεφ.1, σελίδα 8).

Εξ ορισμού της G/p έχουμε

$$G/p=G^{ab}/p$$

Επομένως

$$H_1(\mathbf{Z}/p) =H_1(\mathbf{Z})/p= G^{ab}/p=G/p$$

Συνεπώς $d_1^{(p)}(G)= d^{(p)}(G)$ δηλαδή την αποδεικτέα σχέση του λήμματος.

Λήμμα 3.15

Για κάθε ομάδα G ισχύει

$$\mathbf{d^{(p)}H_2(Z)= d_2^{(p)}G- d_1^{(p)}G.}$$

Απόδειξη

Έχουμε αποδείξει οτι η ακολουθία

$$0\rightarrow H_i(\mathbf{Z})/p \rightarrow H_i(\mathbf{Z}/p)\rightarrow H_{i-1}(\mathbf{Z})_p\rightarrow 0$$

είναι ακριβής. Στην ειδική περίπτωση i=2 προκύπτει η ακρίβεια της ακολουθίας

$$0\rightarrow H_2(\mathbf{Z})/p \rightarrow H_2(\mathbf{Z}/p)\rightarrow H_1(\mathbf{Z})_p\rightarrow 0.$$

Επειδή η G είναι πεπερασμένη έχουμε ότι οι $H_1(\mathbf{Z})/p$, $H_2(\mathbf{Z})/p$ είναι πεπερασμένες ([W] σελ.89]).

Οπότε

$$d_2^{(p)}G= d^{(p)}H_2(\mathbf{Z}/p)= d^{(p)}\ H_2(\mathbf{Z})+\dim_{Fp}H_1(\mathbf{Z})_p$$

Αυτό το βλέπει κανείς εύκολα από την ανάλυση της A σε ευθύ γινόμενο κυκλικών παραγόντων. Επομένως $\dim_{Fp}H_1(\mathbf{Z})_p=\mathbf{F}_p[G] = d_1^{(p)}G$ και συνεπώς $d^{(p)}H_2(\mathbf{Z})= d_2^{(p)}G- d_1^{(p)}G$ δηλαδή το λήμμα.

Χρησιμοποιώντας τα προηγούμενα λήμματα, η ανισότητα

$$¼\ (d^{(p)}G)^2- d^{(p)}G < d^{(p)}\ H_2(\mathbf{Z})$$

γίνεται

$$¼\ (d_1^{(p)}G)^2- d_1^{(p)}G < d_2^{(p)}G- d_1^{(p)}G$$

$$\Leftrightarrow ¼\ (d_1^{(p)}G)^2< d_2^{(p)}G$$

Επομένως αρκεί να αποδείξουμε το θεώρημα:

Θεώρημα 3.16

Έστω G πεπερασμένη p-ομάδα όπου p πρώτος τότε

$$\mathbf{¼\ (d_1^{(p)}G)^2< d_2^{(p)}G.}$$

Για να αποδείξουμε το θεώρημα υπενθυμίζουμε μερικούς συμβολισμούς:

Λ:=$\mathbf{Z}$[G] ο δακτύλιος ομάδος της G

I : το augmentation ιδεώδες του Λ, δηλαδή ο πυρήνας της απεικόνισης

φ :Λ→Λ, με $\varphi(\sum_{\sigma\in G} n_\sigma\sigma)=\sum_{\sigma\in G} n_\sigma$, $I=Ker\varphi=\{\sum_{\sigma\in G} n_\sigma\sigma : \sum_{\sigma\in G} n_\sigma\sigma =0\}$

$\Lambda/p=\mathbf{F}_p[G]=\{\sum_{\sigma\in G} n_\sigma\sigma : n_\sigma\in \mathbf{F}_p\}$

Για την απόδειξη του θεωρήματος θα χρησιμοποιήσουμε τα παρακάτω λήμματα:

Λήμμα 3.17

Έστω G πεπερασμένη p-ομάδα και A ένα G-module με pA=0. Τότε ο ελάχιστος αριθμός γεννητόρων του A ως G-module είναι ίσος με

$$\dim_{F_p} H_0(A)=\dim_{F_p} A/IA.$$

Ειδικά: Έστω $\alpha_i \in A$ ($i\in I$) τότε τα α_i παράγουν το A ως G-module τότε και μόνο τότε οι εικόνες των α_i στο A/IA παράγουν το A/IA ως F_p-διανυσματικό χώρο.

Απόδειξη

Έστω οτι $\overline{a_i}=\alpha_i+IA$ παράγουν τον A/IA ως F_p-διανυσματικό χώρο.

Θέτουμε $B:=<\alpha_1,\alpha_2,\ldots,\alpha_s>$ ένα G-υποmodule του A .

Η φυσική απεικόνιση $\alpha_i+IB\rightarrow\alpha_i+IA$ μας δίνει έναν επιμορφισμό $B/IB\rightarrow A/IA$.

Διότι αν $\overline{a}=a+IA\in A/IA$ τότε $\overline{a}=\sum_{i=1}^{s}\lambda_i\overline{a_i}$, $\lambda_i\in F_p$

Θέτουμε $b=\sum_{i=1}^{s}\lambda_i a_i\in B$, $\lambda_i\in \mathbf{Z}$.

Τότε $\overline{b}\rightarrow\overline{a}$. Η απεικόνιση αυτή επάγει απεικόνιση, έστω φ,

$$H_0(B)\xrightarrow{\phi}H_0(A)$$

η οποία είναι επίσης επί.

Η ακολουθία

$$0\rightarrow B\rightarrow A\rightarrow A/B\rightarrow 0$$

είναι ακριβής και μας δίνει την ακριβή ακολουθία

$$H_0(B)\xrightarrow{\phi}H_0(A)\xrightarrow{\psi}H_0(A/B)\rightarrow 0.$$

Άρα η $\psi:H_0(A)\rightarrow H_0(A/B)$ είναι επί.

Οπότε $H_0(A)=\varphi(H_0(B))=\mathrm{Ker}\psi$. Από αυτά τα δύο συμπεραίνουμε ότι $H_0(A/B)=0$.

Επειδή η ομάδα A/B μηδενίζεται από το p και η G είναι p-ομάδα έχουμε A/B=0 (δες, Κεφ.1 Λήμμα 5.2, σελίδα 13).

Συνεπώς A=B, δηλαδή το λήμμα.

Λήμμα 3.18

Έστω G μια πεπερασμένη p-ομάδα και A ένα G-module με pA=0. Τότε υπάρχει μια επίλυση

$$\ldots\rightarrow Y_2\rightarrow Y_1\rightarrow Y_0\rightarrow A\rightarrow 0$$

τέτοια ώστε:

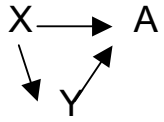
(i)Κάθε Y_n είναι ένα ελεύθερο Λ/p- module.

(ii)Το πλήθος των γεννητόρων του Y_n ως ελεύθερο Λ/p-module είναι ισο με την $\dim_{F_p} H_n(A)$.

(iii)$\mathbf{Im(Y_{n+1})\subseteq IY_n}$.

Απόδειξη

Έστω $d:=\dim_{Fp}H_0(A)$. Από το προηγούμενο λήμμα έπεται ότι υπάρχει ένα ελεύθερο Λ-module X με d γεννήτορες και ένας επιμορφισμός $X \to A$.
Επειδή $pA=0$ ο επιμορφισμός $X \to A$ επάγει έναν επιμορφισμό $X/p \to A$. Θέτουμε $Y:= X/p$.
Το διάγραμμα



είναι αντιμεταθετικό. Το Y=X/p είναι ένα ελεύθερο Λ/p-module με d γεννήτορες ([AW] Th.6 σελ.112). Επομένως, (δες Κεφ.1 Θεώρ. 5.5, σελ. 14), $H_i(Y)=0$ για κάθε $i\geq 1$. Αν B είναι ο πυρήνας του επιμορφισμού $Y \to A$, η ακολουθία

$$0 \to B \to Y \to A \to 0$$

είναι ακριβής.

Συνεπώς έχουμε την ακριβή ακολουθία

$$\ldots \to H_{i+1}(Y) \to H_{i+1}(A) \to H_i(B) \to H_i(Y) \to \ldots$$

Επειδή

$$H_{i+1}(Y)=H_i(Y)=0$$

έπεται ότι

$$H_{i+1}(A)=H_i(B) \text{ για κάθε } i\geq 1.$$

Για i=0 έχουμε λοιπόν την ακριβή ακολουθία

$$\ldots \to H_1(A) \to H_0(B) \to H_0(Y) \to H_0(A) \to 0 \ldots$$

Επειδή

$$H_1(Y)=0$$

έπεται ότι η ακολουθία

$$0 \to H_1(A) \to H_0(B) \to H_0(Y) \to H_0(A) \to 0$$

είναι ακριβής.
Εκ κατασκευής, τα Y και A έχουν το ίδιο πλήθος ελάχιστων γεννητόρων, οπότε από το προηγούμενο λήμμα, έχουμε $\dim H_0(Y)=\dim H_0(A)$, δηλαδή ότι ο επιμορφισμός $H_0(Y) \to H_0(A)$ είναι ισομορφισμός. Αυτό σημαίνει ότι $H_0(B)= H_0(A)$, δηλαδή ότι η σχέση $H_i(B)= H_{i+1}(A)$ ισχύει και για i=0. Λόγω του ισομορφισμού $H_0(Y) \to H_0(A)$ έπεται ότι η απεικόνιση

$$B/IB=H_0(B) \to H_0(Y)=Y/IY$$

είναι η μηδενική, οπότε $B\subseteq IY$.
Αν θέσουμε $Y=Y_0$, έχουμε ότι η ακολουθία

$$Y_0 \to A \to 0, \text{ είναι ακριβής.}$$

Είναι το πρώτο βήμα της επίλυσης την οποία θέλουμε να κατασκευάσουμε.

Εφαρμόζουμε την ίδια διαδικασία για το B.
Θα βρούμε ένα module Y_1 τέτοιο ώστε η ακολουθία $Y_1 \to B \to 0$ να είναι ακριβής με πυρήνα ένα module C για το οποίο ισχύει

$$H_i(C)=H_{i+1}(B)=H_{i+2}(A) \text{ για κάθε } i\geq 0 \text{ και } C \subseteq IY.$$

Το Y_1 είναι ελεύθερο Λ/p-module με $\dim H_0(B)=\dim H_1(A)$ γεννήτορες.
Αν ορίσουμε την απεικόνιση $Y \to Y_0$ να είναι η σύνθεση των $Y_1 \to B \to Y_0$ τότε, επειδή $B \subseteq IY$, θα έχουμε $\mathrm{Im}(Y_1) \subseteq IY_0$.
Συνεχίζουμε, επαγωγικά και αποδεικνύουμε το λήμμα.

Ας εφαρμόσουμε το προηγούμενο λήμμα για A= **Z**/p. Τότε η $H_0(\mathbf{Z}/p)=\mathbf{Z}/p$ έχει διάσταση 1, οπότε Y_0 είναι ελεύθερο module με ένα γεννήτορα. Από την ιδιότητα (iii) του λήμματος 3.18 έπεται ότι ο πυρήνας της $Y_0 \to \mathbf{Z}/p$ περιέχεται στο IY_0. Επειδή Y_0/IY_0 έχει διάσταση 1, άρα ο πυρήνας της απεικόνισης $Y_0 \to \mathbf{Z}/p$ είναι το IY_0. Οπότε η ακολουθία

$$Y_1 \to IY_0 \to 0$$

είναι ακριβής.
Αλλάζοντας τώρα τους συμβολισμούς έχουμε το παρακάτω πόρισμα

Πόρισμα 3.19

Αν G πεπερασμένη p-ομάδα και θέσουμε

$$\mathbf{d=d_1^{(p)}G,\ r=d_2^{(p)}G,}$$

τότε υπάρχει μια ακριβής ακολουθία

$$\mathbf{R \to D \to IE \to 0}$$

με $\mathrm{Im}(R) \subseteq ID$, όπου E, D, R είναι ελεύθερα Λ/p-module με 1, d, r γεννήτορες αντίστοιχα.

Απόδειξη του θεωρήματος 3.16

(Χρησιμοποιούμε τους συμβολισμούς του πορίσματος)
Για κάθε πεπερασμένο G-module A με pA=0, ορίζουμε το πολυώνυμο Poincare

$$P_A(t)=\sum_{0\leq n} c_n(A)\, t^n \text{ όπου } c_n(A)=\dim(I^nA/I^{n+1}A)$$

Έχουμε $c_0(E)=\dim(E/IE)=\dim H_0(E)=1$ (διότι το πλήθος των γεννητόρων είναι 1), οπότε

$$P_E(t)=1+\sum_{n\geq 1} c_n(E)t^n$$
$$=1+t\,c_1(E)+t^2 c_2(E)+\dots$$

Αλλά $c_1(E)=\dim(IE/I^2E)$, $c_2(E)=\dim(I^2E/I^3E)$,…

Άρα

$$P_E(t)=1+t\ c_0(IE)+t^2\ c_1(IE)+\ldots.$$
$$=1+t(c_0(IE)+t\ c_1(IE)+\ldots.)$$
$$=1+tP_{IE}(t)$$

οπότε

$$P_{IE}(t)=(P_E(t)-1)/t.$$

Το D είναι ελεύθερο Λ/p-module με d γεννήτορες, δηλαδή $D=(\Lambda/p)\alpha_1\oplus\ldots\oplus(\Lambda/p)\alpha_d$.

Αλλά $E=\Lambda/p\alpha_i$, άρα $D=E^d$.

Οπότε $c_n(D)=\dim((I^nD)/(I^{n+1}D))=\dim((I^nE)/(I^{n+1}E))^d=d\,c_n(E)$. Άρα έχουμε

$$P_D(t)=dP_E(t)=dP(t).$$

Όμοια $P_R(t)=r.P(t)$.

Γενικά, αν $0<t<1$ είναι πραγματική μεταβλητή, έχουμε

$$P_A(t)(1/(1-t))=\sum_{n\geq 0} s_{n-1}(A)t^n,\ \text{όπου}\ s_{-1}(A)=0.$$

Πράγματι είναι $0<t<1$ άρα $1/1-t=\sum_{n=0}^{\infty} t^n$, άρα

$$P_A(t)(1/(1-t))=(\sum_{n\geq 0} c_n(A)t^n)(\sum_{n=0}^{\infty} t^n)$$
$$=c_0(A)+(c_0(A)+c_1(A))+\ldots$$
$$=\sum_{n\geq 0} s_n(A)t^n,\ \text{όπου}\ s_n(A)=\sum_{0\leq i\leq n} c_i(A)=\dim(A/(I^{n+1}A)).$$

Από το πόρισμα 3.19 υπάρχει επιμορφισμός από G-modules $I^{n+1}D\ \rightarrow I^{n+2}E$ (διότι $D\rightarrow IE$ επιμορφισμός οπότε $I^{n+1}D\rightarrow I^{n+1}(IE)=I^{n+2}(E)$ επιμορφισμός), οπότε η ακριβής ακολουθία

$$R\rightarrow D\rightarrow IE\rightarrow 0$$

μας δίνει μέσω περιορισμού και προβολής την ακριβή ακολουθία

$$0\rightarrow R/R_{n+1}\rightarrow D/I^{n+1}D\rightarrow (IE)/(I^{n+2}E)\rightarrow 0.$$

Οπότε

$$s_n(D)=s_n(IE)+\dim(R/R_{n+1}).$$

Αλλά, από το προηγούμενο πόρισμα, έχουμε οτι $Im(R)\subseteq ID$ οπότε $Im(I^nR)\subseteq I^{n+1}D$ και $Im(I^nR)\subseteq R_{n+1}$.

Επομένως $\dim(R/R_{n+1})\leq\dim(R/I^nR)=s_{n-1}(R)$, οπότε

$$P_D(t)(1/(1-t))\leq P_{IE}(t)\ (1/(1-t))+P_R(t)\ (t/(1-t))$$

ισοδύναμα

$$dP(t)\leq(P(t)-1)/t+rtP(t)\ \text{για}\ 0<t<1$$

δηλαδή

$$1\leq P(t)(rt^2-dt+1),\ \text{για}\ 0<t<1.$$

Θέτουμε t=d/2r (επιτρέπεται, διότι από το λήμμα 3.15, $d \leq r < 2r$ οπότε $0<d/2r<1$).
Άρα

$$r > (1/4)d^2,$$

δηλαδή αποδείξαμε πλήρως το θεώρημα των Golod-Shafarevich.

<u>Σημείωση</u>:
Οι Golod, Shafarevich απέδειξαν μόνο οτι

$$\mathbf{d_2^{(p)}G > 1/4(d_1^{(p)}G-1)^2}$$

Η ανισότητα όπως δόθηκε εδώ αποδείχθηκε ανεξάρτητα από τους Gaschutz και Vinberg.

<u>Απόδειξη του θεωρήματος 3.10 (Brumer) για επεκτάσεις Galois</u>:
Έστω οτι η k/**Q** είναι πεπερασμένη επέκταση Galois με [k:**Q**]=n και p πρώτος αριθμός.
Θα αποδείξουμε την ανισότητα

$$d^{(p)}Cl_k \geq t_k^{(p)}-((r_k-1)/(p-1)+w_p(n)\delta_k^{(p)}) \quad (*)$$

Η απόδειξη θα γίνει σε δυο βήματα, στο πρώτο θα ανάγουμε την ανισότητα σε ένα αποτέλεσμα της Θεωρίας Ομάδων και στο δεύτερο βήμα θα αποδείξουμε το αποτέλεσμα αυτό.
Έστω $K=k_1$ το σώμα του Hilbert του k

G=Gal(K/k),η ομάδα Galois, της επέκτασης K/k
G^*=Gal(K/**Q**), η ομάδα Galois, της επέκτασης K/**Q**
g:=Gal(k/**Q**), η ομάδα Galois, της επέκτασης k/**Q**

Προφανώς η g είναι η ομάδα πηλίκων G^*/G.
Η παρακάτω ακολουθία είναι ακριβής (inflation-restriction), (δες, Κεφ.1, Θεώρ. 3.1, σελίδα 10)

$$1 \rightarrow H^1(g,E_k) \rightarrow H^1(G^*,E_K) \rightarrow H^1(G,E_K).$$

Οπότε

$$d^{(p)}H^1(G^*,E_K) \leq d^{(p)}H^1(G,E_K)+ d^{(p)}H^1(g,E_k).$$

Αρκεί να αποδείξουμε οτι:
(i) $H^1(G,E_K)=Cl_k$
(ii) $d^{(p)}\ H^1(G^*,E_K)=t_k^{(p)}$
(iii) $d^{(p)}\ H^1(g,E_k) \leq (r_k-1)/(p-1)+w_p(n)\delta_k^{(p)}$.

Για κάθε αλγεβρικό σώμα αριθμών K θεωρούμε το ακριβές αντιμεταθετικό διάγραμμα

$$
\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & E_K & \to & U_K & \to & U_K/E_K & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & K^* & \to & U_K & \to & C_K & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & P_K & \to & D_K & \to & Cl_K & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}
$$

Η ακρίβεια των γραμμών και των δυο πρώτων στηλών είναι προφανής. Η ακρίβεια της τρίτης στήλης είναι άμεση συνέπεια του «λήμματος 9» της θεωρίας ομολογίας.
Όπου I_K: η ομάδα των idele του
D_K: η ομάδα των διαιρετών του K
P_K: η ομάδα των κύριων διαιρετών του K
K: η πολλαπλασιαστική ομάδα του K.
Αν K/k είναι Galois με ομάδα Galois G τότε το προηγούμενο διάγραμμα μας δίνει το παρακάτω ακριβές αντιμεταθετικό διάγραμμα.

$$
\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & & & \\
\downarrow & & & & & & \downarrow & & \\
 & & & & & & & &
\end{array}
$$

$$1 \to E_k \to U_k \to (U_K/E_K)^G \xrightarrow{\delta} H^1(E_K) \xrightarrow{\phi} H^1(U_K)$$

$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$

$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$

$$\downarrow$$

$$1 \to k^* \to I_k \to C_k \to H^1(K^*)=1$$

$$\downarrow$$

$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$

$$1 \to P_K{}^G \to D_K{}^G \to Cl_K{}^G$$

$$\downarrow$$

$$\downarrow$$

$$H^1(E_K) \xrightarrow{\phi} H^1(U_K)$$

$$\downarrow$$

$$\downarrow$$

$$1 = H^1(K^*) \quad H^1(I_K) = 1$$

Χρησιμοποιήσαμε δυο φορές το 90^o Θεώρημα του Hilbert: $H^1(K^*)=1$, στο τέλος της πρώτης γραμμής και στο τέλος της δεύτερης γραμμής και μια φορά την $H^1(I_K)=1$ στο τέλος της δεύτερης στήλης (δές, [AW], Cor.7.6, σελ177) ή (δές, [N1], Cor.3.5, σελ.212).

Λήμμα 3.20

Έστω K ένα αλγεβρικό σώμα αριθμών το οποίο είναι επέκταση Galois ως προς κάποιο υπόσωμα k πεπερασμένου βαθμού, με G=Gal(K/k). Υποθέτουμε οτι $D^G{}_K \subseteq P_K$ δηλαδή ότι κάθε G-αναλλοίωτο ιδεώδες του D_K είναι κύριο. Τότε υπάρχει μια ακριβής ακολουθία

$$\mathbf{1 \to Cl_k \to H^1(E_K) \xrightarrow{\phi} H^1(U_K) \to 1.}$$

Απόδειξη

Η φ : $H^1(E_K) \to H^1(U_K)$ εμφανίζεται δύο φορές στο προηγούμενο διάγραμμα. Θα αποδείξουμε ότι η φ είναι επί και kerφ=Cl_k. Από την υπόθεση του λήμματος 3.20 έχουμε ότι $P_K{}^G = D_K{}^G$. Διότι πάντοτε ισχύει $P_K \subseteq D_K$ οπότε και $P_K{}^G \subseteq D_K{}^G$.
Από την άλλη μεριά $(D_K)^G \subseteq P_K$. Συνεπώς $((D_K)^G)^G \subseteq (P_K)^G$ δηλαδή $(D_K)^G \subseteq (P_K)^G$.
Από τις δυο σχέσεις του περιέχεσθαι έπεται η ισότητα $(P_K)^G = (D_K)^G$.
Από το κάτω αριστερό ορθογώνιο του διαγράμματος τώρα συμπεραίνουμε ότι η φ είναι επιμορφισμός. Από την προτελευταία γραμμή του διαγράμματος συμπεραίνουμε επίσης ότι α=1. Δηλαδή,

$$\begin{array}{ccc} (P_K)^G & \xrightarrow{1-1} & (D_K)^G = (P_K)^G \\ \text{επί}\downarrow & & \downarrow\text{επί} \\ H^1(E_K) & \xrightarrow{\phi} & H^1(U_K) \end{array}$$

Η αντιμεταθετικότητα του διαγράμματος :

$$\begin{array}{ccc} & & I_k \xrightarrow{n} C_k \\ & \downarrow & \downarrow \\ (D_k)^G & \xrightarrow{a} & (Cl_k)^G \end{array}$$

μας δίνει ότι α∘ξ=β∘η=1. Επειδή ο η είναι επιμορφισμός έπεται ότι β=1. Αυτό σημαίνει ότι ο γ είναι κατ΄ ανάγκη ισομορφισμός.

Οπότε, από την δεξιά πάνω γωνία του διαγράμματος, έχουμε

$$\text{Ker}\varphi = \text{Im}(\delta) = (U_K/E_K)^G/\text{Im}(\varepsilon) = C_k/\text{Im}(\gamma \circ \varepsilon)$$

διότι ο γ είναι ισομορφισμός.

Από την άλλη μεριά όμως $(C_k/(Im(\gamma o \varepsilon)))= (C_K/(Im(\eta o \zeta)))=I_k/kU_k=Cl_k$ δηλαδή το ζητούμενο $ker\varphi=Cl_k$.

Απόδειξη του (i)

Υπενθυμίζουμε ότι k είναι το σώμα Hilbert του σώματος k. Το Θεώρημα των κύριων ιδεωδών (Principal ideal Theorem) είναι το:

«Κάθε ιδεώδες του k όταν επεκταθεί στο σώμα του Hilbert γίνεται κύριο, δηλαδη $D_k \subseteq P_K$».

Την εποχή που τέθηκε το πρόβλημα του πύργου κλάσεων σωμάτων ήταν και αυτό εικασία. Αποδείχθηκε όμως πολύ νωρίτερα, στα 1930 από τον Furtwangler (δες, [N2], Prop. , σελίδα)

Επειδή K/k μη διακλαδιζόμενη έχουμε $H^1(U_K)=1$. Θα δείξουμε οτι το K ικανοποιεί τις προυποθέσεις του Λήμματος 3.20, δηλαδή οτι $(D_K)^G \subseteq P_K$.

Επειδή $H^1(U_K)=1$, από το προηγούμενο διάγραμμα, έχουμε οτι η απεικόνιση $\xi: I_K \rightarrow (D_K)^G$ είναι επί. Η εικόνα όμως της ξ είναι $I_k/U_k=D_k$. Επομένως $D_k=(D_K)^G$ οπότε $(D_K)^G \subseteq P_K$.

Εφαρμόζουμε τώρα το προηγούμενο λήμμα 3.20. Η ακολουθία

$$1 \rightarrow Cl_k \rightarrow H^1(E_K) \xrightarrow{\phi} H^1(U_K) \rightarrow 1$$

είναι ακριβής. Επειδή $H^1(U_K)=1$ έπεται ότι $Cl_k= H^1(E_K)$, δηλαδή η (i).

Απόδειξη της (ii)

Θα αποδείξουμε οτι η επέκταση K/**Q** ικανοποιεί τις προϋποθέσεις του προηγούμενου λήμματος (το K είναι και πάλι το σώμα του Hilbert του k). Υπενθυμίζουμε ότι η G* είναι η ομάδα Galois της επέκτασης K/**Q** και G η ομάδα Galois της επέκτασης K/ k, άρα $G \subseteq G^*$, οπότε $(D_K)^{G^*} \subseteq (D_K)^G$.

Αλλά από την απόδειξη της (i) έχουμε $(D_K)^G \subseteq P_K$, οπότε και $(D_K)^{G^*} \subseteq P_K$.

Άρα από το προηγούμενο λήμμα 3.20 έχουμε:

$$1 \rightarrow Cl_{\mathbf{Q}} \rightarrow H^1(G^*,E_K) \xrightarrow{\phi} H^1(G^*,U_K) \rightarrow 1.$$

Λόγω του ότι $Cl_{\mathbf{Q}}=1$, η παραπάνω ακριβής ακολουθία μας δίνει ότι η φ

$$H^1(G^*,E_K) \xrightarrow{\phi} H^1(G^*,U_K)$$

είναι ισομορφισμός.

Για κάθε πεπερασμένο πρώτο $q \in \mathbf{Q}$ θέτουμε $e_K(q)$=ο δείκτης διακλάδωσης κάποιας επέκτασης του q στο K (επειδή η K/**Q** είναι Galois το e(q) δεν

εξαρτάται από την επιλογή της επέκτασης). Έστω $\mathbf{Z}/e_K(q)$ η κυκλική ομάδα τάξεως $e_K(q)$, τότε $H^1(G^*,U_K)=\prod_q \mathbf{Z}/e_K(q)$.

Επειδή K/k είναι μη διακλαδιζόμενη επέκταση έχουμε ότι $e_K(q)=e_k(q)$ για κάθε πεπερασμένο πρώτο q του **Q**.
Οπότε $H^1(G^*,E_K)= \prod_q Z/e_k(q)$.

Ο p-rang του γινομένου στο δεξί μέλος είναι ίσος με το πλήθος των q τέτοιων ώστε $p/e_k(q)$, δηλαδή ίσος με $t_k^{(p)}$. Συνεπώς έχουμε αποδείξει ότι $d^{(p)}H^1(G^*,E_K)=t_k^{(p)}$.

Απόδειξη της (iii)
Η torsion ομάδα της E_k είναι η W_k η οποία είναι κυκλική με p-rank $\delta_k^{(p)}$ (Θεώρημα Μονάδων του Dirichlet). Αλλά από το Θεώρημα των Μονάδων η E_k/W_k είναι ελεύθερη αβελιανή ομάδα με (r_k-1) γεννήτορες. Οπότε η (iii) είναι άμεση συνέπεια του παρακάτω αποτελέσματος της Θεωρίας Ομάδων.

Λήμμα 3.21
Έστω G μια πεπερασμένη ομάδα τάξης n και p ένας πρώτος αριθμός. Έστω A ένα πεπερασμένα παραγόμενο G-module με torsion ομάδα tA και έστω ρ(A) ο αριθμός των ελεύθερων γεννητόρων του A/tA ως αβελιανή ομάδα, τότε

$$\mathbf{d^{(p)}H^1(G,A)\le(\rho(A)/p-1)+w_p(n)d^{(p)}tA.}$$

Απόδειξη
Έστω $H^1(G,A) \to H^1(G^{(p)},A)$ ο περιορισμός (restriction), όπου $G^{(p)}$ είναι μια p-Sylow υποομάδα της G.Η προηγούμενη απεικόνιση είναι μονομορφισμός των p-primary συνιστώσων (δές, [AW], Prop.8, Cor.3, σελ.105).
Ειδικά $d^{(p)}H^1(G,A)\le d^{(p)}H^1(G^{(p)},A)$.
Οπότε αρκεί να αποδείξουμε το λήμμα για την ομάδα $G^{(p)}$ η οποία είναι p-ομάδα (Ισχύει $w_p(n)=w_p(n^{(p)})$ όπου $n^{(p)}$ η τάξη της $G^{(p)}$). Η ακολουθία

$$0 \to tA \to A \to A/tA \to 0$$

είναι ακριβής, οπότε και η ακολουθία

$$H^1(G,tA) \to H^1(G,A) \to H^1(G,A/tA)$$

θα είναι επίσης ακριβής. Οπότε

$$d^{(p)}H^1(G,A)\le d^{(p)}H^1(G,tA)+ d^{(p)}H^1(G,A/tA).$$

Θα αποδείξουμε ότι

$$d^{(p)}H^1(G,tA)\le w_p(n)d^{(p)}tA$$

και $d^{(p)}H^1(G,A/tA)\le \rho(A)/(p-1)$
Διακρίνουμε δυο περιπτώσεις:

$1^{η}$ περίπτωση: Το A είναι torsion module
$2^{η}$ περίπτωση: Το A είναι torsion free

$1^{η}$ περίπτωση: Έχουμε $d^{(p)}G=\dim G/p \le w_p(n)$.
Οπότε αρκεί να δείξουμε οτι $d^{(p)}H^1(A) \le d^{(p)}Gd^{(p)}A$.
Έστω $Z^1(A)$ το module των σταυρωτών ομομορφισμών $f : G \to A$.
Έστω $g_1,g_2,\ldots,g_d$ ένα ελάχιστο σύστημα γεννητόρων της G. Το Θεώρημα Βασης του Burnside για τις p-ομάδες μας λέει οτι

$$d=d^{(p)}G.$$

Κάθε σταυρωτός ομομορφισμός f ορίζεται μονοσήμαντα από τις τιμές των $f(g_i)$ $1 \le i \le d$, δηλαδή η απεικόνιση

$$Z^1(A) \to A^d$$

με $f \to (f(g_1),\ldots f(g_d))$ είναι 1-1.
Οπότε

$$d^{(p)}Z^1(A) \le d^{(p)}(A^d)=dd^{(p)}(A)= d^{(p)}(G)d^{(p)}(A)$$

Επειδή το $H^1(A)$ είναι πηλίκο της $Z^1(A)$ έχουμε

$$d^{(p)}H^1(A) \le d^{(p)}Z^1(A) \le d^{(p)}(G) d^{(p)}(A).$$

Σημείωση
Στην παραπάνω απόδειξη δεν χρησιμοποιούμε το γεγονός οτι η A είναι torsion module. Επομένως η ανισότητα ισχύει για κάθε πεπερασμένα παραγόμενο G-module A.
Αυτό σημαίνει οτι αποδείξαμε το εξης

$$d^{(p)}H^1(g,E_k) \le w_p(n)(r_k-1+\delta_k^{(p)})$$

και αντί της (*) την

$$d^{(p)}Cl_k \ge t_k^{(p)}-w_p(n)(r_k-1+\delta_k^{(p)})$$

Αυτό είναι αρκετό για να πάρουμε μια συνάρτηση c΄(n) με

$$d^{(p)}Cl_k \ge t_k^{(p)}-c'(n)$$

και επειδή $w_p(n) \le n-1$ μπορούμε να πάρουμε $c'(n)=(n-1)n$.

Η απόδειξη που ακολουθεί μας επιτρέπει να δώσουμε μια καλύτερη εκτίμηση στην περίπτωση που το module είναι torsion free. Θα αποδείξουμε ότι μπορούμε να πάρουμε $c'(n)=2(n-1)$.

$2^{η}$ περίπτωση: Το A είναι torsion free

Λήμμα 3.22 (Chevalley)

Έστω G μια ομάδα τάξης p και A ένα πεπερασμένα παραγόμενο G-module
Τότε

$$\mathbf{d^{(p)}H^1(G,A)- d^{(p)}H^2(G,A)=(\rho(A)-p\rho(A))/(p-1).}$$

Απόδειξη

(i) Έστω $d_{1-2}(A)=d^{(p)}H^1(G,A)-d^{(p)}H^2(G,A)$

Επειδή η G έχει τάξη p έχουμε $p.H^i(A)=0$ [AW]

Επομένως $d^{(p)}H^i(A)=\dim H^i(A)$ ως $\mathbf{F}_P$ διανυσματικό χώρο. Αν τώρα με $h^i(A)$ συμβολίσουμε την τάξη της $H^i(A)$, τότε

$$h^i(A)=p^{d^{(p)}H^i(A)}$$

Το πηλίκο του Herbrant

$$h_{1/2}= h^1(A)/ h^2(A)$$

Άρα

$$h_{1/2}=p^{d_{1-2}(A)}$$

Από τις ιδιότητες του πηλίκου του Herbrant (Κεφ.1 Προτ.2.2) έχουμε ότι

$$h_{1/2}(B)= h_{1/2}(A)\, h_{1/2}(C)$$

οπότε

$$d_{1-2}(B)= d_{1-2}(A).d_{1-2}(C)$$

δηλαδή η d_{1-2} είναι μια προσθετική συνάρτηση από G-modules.

Ορισμός 3.23

Δυο πεπερασμένα γεννόμενα G-modules A και B λέγονται ρητά ισοδύναμα αν τα τανυστικά γινόμενα $A\otimes Q$ και $B\otimes Q$ είναι ισόμορφα ως Q[G]-modules, όπου $Q[G]=Z[G]\otimes G$ ο δακτύλιος ομάδας της G υπέρ το Z.

Γνωρίζουμε οτι:

«Αν A και B είναι ρητά ισοδύναμα τότε $d_{1-2}A=d_{1-2}B$ »

οπότε λέμε οτι η d_{1-2} είναι μια συνάρτηση ρήτων ισοδύναμων κλάσεων.

Ορίζουμε την συνάρτηση

$$\tau(A)=(\rho(A)-p\rho(A^G))/(p-1).$$

Η τ είναι μια προσθετική συνάρτηση ρητών ισοδυνάμων κλάσεων.

Για να το αποδείξουμε αυτό αρκεί να αποδείξουμε οτι οι συναρτήσεις ρ(A), $\rho(A^G)$ είναι προσθετικές. Πράγματι από τον ορισμό της ρ έχουμε $\rho(A)=\dim_{\mathbf{Q}}A\otimes\mathbf{Q}$.

Αν η ακολουθία

$$0\to A\to B\to C\to 0$$

είναι ακριβής τότε και η ακολουθία

$$0 \to A\otimes \mathbf{Q} \to B\otimes \mathbf{Q} \to C\otimes \mathbf{Q} \to 0$$

είναι ακριβής, οπότε

$$\dim B\otimes \mathbf{Q}=\dim A\otimes \mathbf{Q}+\dim A\otimes \mathbf{Q},$$

δηλαδή ρ(B)=ρ(A)+ρ(C), άρα η ρ είναι προσθετική.

Είναι $\rho(A^G)=\dim_{\mathbf{Q}}(A^G\otimes \mathbf{Q})=\dim_{\mathbf{Q}}(A\otimes \mathbf{Q})^G$ διότι το **Q** μπορούμε να το θεωρήσουμε ως G-module με τετριμμένη δράση δηλαδή $\mathbf{Q}^G=\mathbf{Q}$ οπότε $A^G\otimes \mathbf{Q}= A^G\otimes \mathbf{Q}^G= (A\otimes \mathbf{Q})^G$.

Οπότε αν η ακολουθία

$$0 \to A \to B \to C \to 0$$

είναι ακριβής τότε και η ακολουθία

$$0 \to (A\otimes \mathbf{Q})^G \to (B\otimes \mathbf{Q})^G \to (C\otimes \mathbf{Q})^G \to 0$$

είναι ακριβής, διότι $H^1(G, A\otimes \mathbf{Q})=0$ αφού $A\otimes \mathbf{Q}$ είναι uniquely divisible.

Άρα

$$\dim(B\otimes \mathbf{Q})^G=\dim(A\otimes \mathbf{Q})^G+\dim(A\otimes \mathbf{Q})^G$$

επομένως

$$\rho(B^G)= \rho(A^G)+ \rho(C^G)$$

δηλαδή $\rho(A^G)$ προσθετική.

Ισχύουν

$$d_{1\text{-}2}(\mathbf{Z})=\tau(\mathbf{Z})=-1$$

και $d_{1\text{-}2}(\Lambda)=\tau(\Lambda)=0$

όπου θεωρούμε τα **Z**, Λ=**Z**(G) ως G-module.

Διότι $h_{1/2}(\mathbf{Z})=h^1(\mathbf{Z})/h^2(\mathbf{Z})=\#H^1(\mathbf{Z})/\#H^2(\mathbf{Z})= \#H^1(\mathbf{Z})/\#H^0(\mathbf{Z})=1/p=p^{-1}$ αφού $H^0(\mathbf{Z})=\mathbf{Z}/p\mathbf{Z}$ και $H^1(\mathbf{Z})=(0)$, άρα $d_{1\text{-}2}(\mathbf{Z})=1$.

Για να αποδείξουμε το Λήμμα 3.22 αρκεί να αποδείξουμε την ακόλουθη πρόταση

«Κάθε προσθετική συνάρτηση f ρητών κλάσεων ισοδυναμίας ενός πεπερασμένα παραγόμενου G-module A είναι μονοσήμαντα ορισμένη από τις τιμές της στα **Z** , Λ.»

Απόδειξη

Η ακριβής ακολουθία

$$0 \to I \to \Lambda \to \mathbf{Z} \to 0$$

δείχνει οτι f(I)=f(Λ)-f(**Z**), οπότε το f(I) ορίζεται από τα f(Λ) και f(**Z**). Αυτό που μένει να δείξουμε είναι οτι κάθε πεπερασμένα παραγόμενο G-module A είναι ρητά ισοδύναμο με το ευθύ άθροισμα G-modules τα οποία είναι ισομορφικά είτε με το Z είτε με το I. Δηλαδή

$$A\otimes \mathbf{Q}=\sum_i A_i\otimes \mathbf{Q}$$

όπου $A_i=\mathbf{Z}$ ή $A_i=I$.

Επειδή το $A\otimes \mathbf{Q}$ είναι ένας χώρος αναπαράστασης της G πάνω από το **Q**, το $A\otimes \mathbf{Q}$ είναι ένα ευθή άθροισμα irreducible χώρων αναπαράστασης V_i

δηλαδή θα δειξουμε οτι κάθε irreducible χώρος αναπαράστασης V (διάφορος του μηδενικού) της G πάνω από το **Q** είναι είτε ισομορφικός με το $Z\otimes \mathbf{Q}=\mathbf{Q}$ ή με το $I\otimes \mathbf{Q}$.
Κάθε τέτοιο V είναι ισομορφικό με ένα ευθύ άθροισμα των $\mathbf{Q}(G)=\Lambda\otimes \mathbf{Q}$.
Οπότε πρέπει να ορίσουμε την ανάλυση σε ευθύ άθροισμα των **Q**(Z).
Η ακριβής ακολουθία

$$0 \to I\otimes \mathbf{Q} \to \mathbf{Q}(\mathbf{Z}) \to \mathbf{Q} \to 0$$

είναι διασπώμενη. Η αντίστοιχη απεικόνιση $\mathbf{Q} \to \mathbf{Q}(G)$ ορίζεται $x\to xe$ ($x\in \mathbf{Q}$) όπου $e :=(1/p)\sum_{g\in G} g$.
Οπότε έχουμε την ευθεία ανάλυση $\mathbf{Q}(G)=(I\otimes \mathbf{Q})\oplus \mathbf{Q}e$. Μένει να αποδείξουμε οτι $I\otimes \mathbf{Q}$ είναι ανάγωγο για παράδειγμα ότι ο $I\otimes \mathbf{Q}$ ως **Q**-άλγεβρα είναι σώμα.
Έστω K το σώμα των p ριζών της μονάδας. Έστω χ ένας ισομορφισμός της G στην ομάδα των p ριζών της μονάδας (μέσα στο K) .Επειδή ο χ είναι γραμμικός επεκτείνεται μοναδικά σε μια άλγεβρα ομομορφική του **Q**(G) πάνω στο K. Ο πυρήνας της χ περιέχει το e διότι το άθροισμα όλων των p ριζών της μονάδας στο K είναι μηδέν. Άρα η χ ορίζει μια άλγεβρα ομομορφική του $\mathbf{Q}(G)/e= I\otimes \mathbf{Q}$ πάνω στο K.
Επειδή $\dim_{\mathbf{Q}}K=p-1=\dim_{\mathbf{Q}} I\otimes \mathbf{Q}$ έχουμε οτι είναι ισομορφισμός από το $I\otimes \mathbf{Q}$ πάνω στο K.

<u>Λήμμα 3.24</u>
Έστω G μια πεπερασμένη p-ομάδα και A ένα πεπερασμένα παραγόμενο G-module το οποίο ως αβελιανή ομάδα είναι torsion free. Τότε

$$\mathbf{d^{(p)}H^1(A)\le (\rho(A)-\rho(A^G))/(p-1).}$$

Ειδικά έχουμε ότι

$$\mathbf{d^{(p)}H^1(A)\le \rho(A)/(p-1).}$$

Απόδειξη

Έστω οτι η G έχει τάξη p. Τότε από το Λήμμα του Chevalley έχουμε

$$d^{(p)}H^1(G,A) \le(\rho(A)-p\rho(A))/(p-1)+ d^{(p)}H^2(G,A)$$

Επειδή η G είναι κυκλική, $H^2(A)=H^0(A)$ είναι κάποια ομάδα πηλίκο της A^G οπότε

$$d^{(p)}H^2(A)\le d^{(p)}A^G=\rho(A^G)$$

η τελευταία ισότητα ισχύει διότι η A^G είναι torsion free.
Επομένως,

$$d^{(p)}H^1(G,A) \le(\rho(A)-p\rho(A))/(p-1)+\rho(A^G)$$

το οποίο αποδεικνύει το λήμμα στην περίπτωση που η τάξη της G είναι p.
Έστω τώρα ότι η G έχει τάξη μεγαλύτερη ή ίση του p^2.
Έστω U μια γνήσια κανονική υποομάδα της G. Έχουμε την ακριβή ακολουθία (δες, Κεφ.1, Θεώρημα 3.1)

$$1 \to H^1(G/U,A^U) \to H^1(G,A) \to H^1(U,A)$$

Οπότε

$$d^{(p)}H^1(G,A) \leq d^{(p)}H^1(G/U,A^U) + d^{(p)}H^1(U,A)$$

Χρησιμοποιώντας επαγωγή, υποθέτουμε ότι η σχέση που θέλουμε να αποδείξουμε ισχύει για ομάδες τάξης μικρότερης της G. Επομένως

$$d^{(p)}H^1(G/U,A^U) \leq (\rho(A^U)-\rho(A^G))/(p-1)$$

και

$$d^{(p)}H^1(U,A) \leq (\rho(A)-\rho(A^U))/(p-1)$$

Οπότε, προσθέτοντας κατά μέλη, έχουμε το ζητούμενο.

Βιβλιογραφία

[Α1] Γ.Α. Αντωνιάδη, Συνομολογία Ομάδων, Σημειώσεις, Ηράκλειο 1993.

[Α2] Γ.Α. Αντωνιάδη, Αλγεβρική Θεωρία Αριθμών, Σημειώσεις, Ηράκλειο 1987.

[Α3] Γ.Α. Αντωνιάδη, Εκτιμήσεων-Τοπικά Σώματα, Σημειώσεις, Ηράκλειο 1992.

[AW] M.F. Atiyah and C.T.C.Wall, Cohomology of Groups. Άρθρο από το βιβλίο του [CF].

[CF] J.W.S. Cassels and A.Frohlich, Algebraic Number Theory, Academic Press, London 1967.

[HA] I.N.Herstein, Topics in Ring Theory, The University of Chicago Press, Chicago 1972.

[H] H.Hasse, Vorlesungen uber Klassenkorpertheorie, Physica-Verlag, Wurtzburg 1967.

[Λ] Κ. Λάκκη, Άλγεβρα, Θεσσαλονίκη 1993.

[N1] Jurgen Neukirch, Klassenkorpertheorie , Bibliographishes Institut, Mannheim 1969.

[N2] Jurgen Neukirch, Class Field Theory, Springer-Verlag, Berlin 1986.

[ST] I.N.Stewart and D.O.Tall, Algebraic Number Theory, Chapman and Hall, London 1989.

[S] J.P. Serre, Galois Cohomology, Springer Verlag, Berlin 1997.

[ST] I.N.Stewart and D.O.Tall, Algebraic number Theory, Chapman and Hall, London 1989.

[SH] S.S. Shatz, Profinite Groups, Arithmetic Geometry, Annals of Mathematical Studies, Princeston University Press, Princeston 1972.
[W] E.Weiss, Cohomology of Groups, Academic Press, 1969.