Το Θεώρημα Των Πρώτων Αριθμών Σε Σώματα Συναρτήσεων

Μεταπτυχιακή Εργασία

Γιώργος Ν. Καπετανάκης

Τμήμα Μαθηματικών
Πανεπιστήμιο Κρήτης

10 Απριλίου 2009

επιβλέπων καθηγητής
Θεόδουλος Γαρεφαλάκης

Περιγραφή

1. Σώματα συναρτήσεων
   - Πρώτοι
   - Διαιρέτες
2. Το θεώρημα Riemann-Roch
   - Μερικές συνέπειες του θεωρήματος Riemann-Roch
3. Επεκτάσεις σωμάτων συναρτήσεων
   - Επεκτάσεις σταθερού σώματος
4. Η συνάρτηση ζ του Riemann
   - Το θεώρημα Hasse-Weil
   - Το θεώρημα των πρώτων αριθμών

Σώμα συναρτήσεων

Ορισμός

Έστω K σώμα και F επέκτασή του. Αν υπάρχει $x \in F$, με x μη αλγεβρικό πάνω από το K, τέτοιο ώστε η επέκταση $F/K(x)$ να είναι πεπερασμένη, τότε ονομάζουμε την επέκταση F/K *σώμα συναρτήσεων* (function field). Το σώμα $\overline{K}^F$ είναι το *σώμα σταθερών* του F/K.

- Αν $F = K(x)$, τότε έχουμε το *ρητό* σώμα συναρτήσεων.
- Αν $K = \mathbb{F}$, (με $\mathbb{F}$ πεπερασμένο), τότε έχουμε το *ολικό* (global) σώμα συναρτήσεων.

Σημείωση: Δεχόμαστε ότι $K = \overline{K}^F$.

Διακριτή αποτίμηση

Ορισμός

Έστω F/K σ.σ.. Λέμε ότι μια συνάρτηση $u : F \to \mathbb{Z} \cup \{\infty\}$ είναι *διακριτή αποτίμηση* αν ικανοποιεί τις παρακάτω ιδιότητες.

1. $u(x) = \infty \iff x = 0$.
2. $u(xy) = u(x) + u(y)$ για κάθε $x, y \in F$.
3. $u(x+y) \geq \min\{u(x), u(y)\}$ για κάθε $x, y \in F$.
4. Υπάρχει $z \in F$ τέτοιο ώστε $u(z) = 1$.
5. $u(a) = 0$ για κάθε $a \in K \setminus \{0\}$.

Η ιδιότητα 3 ονομάζεται *τριγωνική ανισότητα*.

Λήμμα (Ισχυρή Τριγωνική Ανισότητα)

Έστω u διακριτή αποτίμηση του σ.σ. F/K και $x, y \in F$ με $u(x) \neq u(y)$. Τότε $u(x+y) = \min\{(u(x), u(y)\}$.

Δακτύλιοι αποτίμησης

Ορισμός

Ένας *δακτύλιος αποτίμησης* (valuation ring) του σ.σ. F/K είναι ένας δακτύλιος $\mathcal{O}$, για τον οποίο $K \subsetneqq \mathcal{O} \subsetneqq F$ και αν $z \in F$, τότε $z \in \mathcal{O}$ ή $z^{-1} \in \mathcal{O}$.

Αν ο $\mathcal{O}$ είναι δακτύλιος αποτίμησης του F/K, τότε

1. ο $\mathcal{O}$ είναι τοπικός δακτύλιος,
2. αν P το (μοναδικό) μεγιστικό ιδεώδες του, τότε το P είναι κύριο και
3. αν $P = t\mathcal{O}$, τότε κάθε $z \in F \setminus \{0\}$ έχει μοναδική αναπαράσταση της μορφής $z = t^n u$, με $n \in \mathbb{Z}$ και $u \in \mathcal{O}^*$.

Πρώτοι

Ορισμός

Ένας *πρώτος* (prime ή place) P του σ.σ. F/K είναι το μεγιστικό ιδεώδες κάποιου δακτύλιου αποτίμησης. Με $\mathbb{P}_F$ συμβολίζουμε το σύνολο των πρώτων του F/K.

1. Οι δακτύλιοι αποτίμησης και οι πρώτοι βρίσκονται σε 1-1 αντιστοιχία.
2. Έχει νόημα ο όρος *δακτύλιος αποτίμησης του πρώτου* P και ο συμβολισμός
$$\mathcal{O}_P := \{z \in F \mid z^{-1} \notin P\}.$$
3. Το P είναι μεγιστικό ιδεώδες του $\mathcal{O}_P$, άρα το ${}^{\mathcal{O}_P}/_{P}$ είναι σώμα. Ακόμα $P \cap K = \{0\}$ και αφού $K \subseteq \mathcal{O}_P$ το K θα είναι υπόσωμα του ${}^{\mathcal{O}_P}/_{P}$.
4. Υπάρχουν άπειροι το πλήθος πρώτοι.

Μεγέθη που χαρακτηρίζουν τους πρώτους

Ορισμός

Έστω $P \in \mathbb{P}_F$. Ορίζουμε ως *τάξη* στον P τη συνάρτηση $\mathrm{ord}_P : F \to \mathbb{Z} \cup \{\infty\}$, που αν $P = t\mathcal{O}$, $z \in F \setminus \{0\}$ και $z = t^n u$, με $u \in \mathcal{O}_P^*$, τότε $\mathrm{ord}_P(z) := n$, και $\mathrm{ord}_P(0) := \infty$.

- Από τα προηγούμενα, ο ορισμός της τάξης είναι καλός.
- Η συνάρτηση ord_P είναι διακριτή αποτίμηση του F/K.

Ορισμός

Έστω $P \in \mathbb{P}_F$, ο αριθμός $\deg P := \left[{}^{\mathcal{O}_P}/{}_{P} : K\right]$ ονομάζεται *βαθμός* του P.

- Από τα προηγούμενα, ο ορισμός του βαθμού είναι καλός.
- Αν $P \in \mathbb{P}_F$ και $x \in P \setminus \{0\}$, τότε

$$\deg P \leq [F : K(x)] < \infty.$$

Διαιρέτες

Ορισμός

Η ελεύθερη αβελιανή ομάδα που παράγεται από τους πρώτους ενός σ.σ. ονομάζεται *ομάδα διαιρετών* (divisor group) και συμβολίζεται ως $\mathcal{D}_F$. Τα στοιχεία της ομάδας διαιρετών ονομάζονται *διαιρέτες* (divisors).

- Ο τυχαίος διαιρέτης είναι ένα τυπικό άθροισμα της μορφής
$$D = \sum_{P \in \mathbb{P}_F} a_P P$$
με $a_P \in \mathbb{Z}$ και $a_P = 0$ για σχεδόν όλους τους P.
- Ως *τάξη* του D στον P (συμβ. $\operatorname{ord}_P(D)$) ονομάζουμε το a_P.
- Μπορεί να οριστεί μερική διάταξη με τον προφανή τρόπο.
- Ως *βαθμό* του διαιρέτη D ορίζουμε τον αριθμό
$$\deg_F D := \sum_{P \in \mathbb{P}_F} \operatorname{ord}_P(D) \cdot \deg P.$$

Ορισμός

Έστω $x \in F \setminus \{0\}$. Ορίζουμε ως

- *διαιρέτη ριζών* του x τον
$$(x)_0 := \sum_{\mathrm{ord}_P(x)>0} \mathrm{ord}_P(x)P,$$
- *διαιρέτη πόλων* του x τον
$$(x)_\infty := \sum_{\mathrm{ord}_P(x)<0} (-\mathrm{ord}_P(x))P \text{ και ως}$$
- *κύριο διαιρέτη* του x τον $(x) := (x)_0 - (x)_\infty$.

Σημείωση: Οι ορισμοί είναι καλοί, αφού αν $x \in F \setminus \{0\}$, τότε $\mathrm{ord}_P(x) > 0$ και $\mathrm{ord}_P(x) < 0$ για πεπερασμένα το πλήθος $P \in \mathbb{P}_F$.

Θεώρημα

Για $x \in F \setminus K$ *ισχύει ότι* $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$.

Πόρισμα

Αν $x \in F \setminus \{0\}$, *τότε* $\deg(x) = 0$.

Ορισμός

- Το σύνολο $\mathcal{P}_F := \{\, (x) \mid x \in F \setminus \{0\} \,\}$ ονομάζεται *ομάδα κύριων διαιρετών* (group of princpal divisors) του F/K.
- Η πηλικοομάδα $\mathcal{C}_F := {}^{\mathcal{D}_F}/_{\mathcal{P}_F}$ ονομάζεται *ομάδα κλάσεων διαιρετών*.
- Δύο διαιρέτες $D, D' \in \mathcal{D}_F$ ονομάζονται *ισοδύναμοι* αν $[D] = [D']$ (συμβ. $D \sim D'$).

Σημείωση: Οι παραπάνω ορισμοί είναι καλοί.

$\mathcal{L}$ χώροι

Ορισμός

Αν $A \in \mathcal{D}_F$, τότε $\mathcal{L}(A) := \{\, x \in F \mid (x) \geq -A \,\} \cup \{0\}$.

Πρόταση

Έστω $A \in \mathcal{D}_F$. Τότε

1. *το $\mathcal{L}(A)$ είναι πεπερασμένης διάστασης K-διανυσματικός χώρος,*
2. *αν $A' \in \mathcal{D}_F$ με $A' \sim A$, τότε $\mathcal{L}(A) \cong \mathcal{L}(A')$ ως διανυσματικοί χώροι,*
3. *$\mathcal{L}(0) = K$ και*
4. *αν $A < 0$ τότε $\mathcal{L}(A) = \{0\}$.*

Διάσταση

Ορισμός

Αν $A \in \mathcal{D}_F$, ο ακέραιος $l(A) := \dim_K \mathcal{L}(A)$ ονομάζεται *διάσταση* του A.

- Αν $A, A' \in \mathcal{D}_F$ με $A \sim A'$, τότε $l(A) = l(A')$ και $\deg A = \deg A'$.
- Αν $A \in \mathcal{D}_F$ με $\deg A \leq 0$ τότε $l(A) = 0$ εκτός αν $A \sim 0$, οπότε $l(A) = 1$.

Το γένος

Πρόταση

Υπάρχει κάποια σταθερά $\gamma \in \mathbb{Z}$ *τέτοια ώστε για κάθε* $A \in \mathcal{D}_F$ *να ισχύει*

$$\deg A - l(A) \leq \gamma.$$

Ορισμός

Το *γένος* (genus) του σ.σ. F/K ορίζεται ως

$$g := \max\{\deg A - l(A) + 1 \mid A \in \mathcal{D}_F\}.$$

- Ο ορισμός είναι καλός.
- Αν g το γένος του F/K, τότε $g \geq 0$.
- (Ανισότητα Riemann) Για κάθε διαιρέτη A έχουμε ότι

$$l(A) \geq \deg A + 1 - g.$$

Το θεώρημα Riemann-Roch

Θεώρημα (Riemann-Roch)

Υπάρχει μια κλάση $\mathcal{W}_F \in \mathcal{C}_F$ τέτοια ώστε αν $W \in \mathcal{W}_F$, τότε για κάθε $A \in \mathcal{D}_F$ να ισχύει ότι

$$l(A) = \deg A + 1 - g + l(W - A).$$

- Η κλάση $\mathcal{W}_F$ ονομάζεται *κανονική κλάση* (canonical class).
- Ένας $W \in \mathcal{W}_F$ ονομάζεται *κανονικός διαιρέτης* (canonical divisor).

Συνέπειες του Riemann-Roch

Πρόταση

Αν $W \in \mathcal{W}_F$, *τότε* $\deg W = 2g - 2$ *και* $l(W) = g$.

Πρόταση

Αν $\deg W = 2g - 2$ *και* $l(W) \geq g$, *τότε* $W \in \mathcal{W}_F$.

Θεώρημα (Riemann)

Αν g *το γένος του* F/K *και* $A \in \mathcal{D}_F$ *με* $\deg A \geq 2g - 1$, *ισχύει ότι*

$$l(A) = \deg A + 1 - g.$$

Σημείωση: Το φράγμα του θεωρήματος Riemann δεν βελτιώνεται, π.χ. για $A \in \mathcal{W}_F$.

Επεκτάσεις

Ορισμός

Αν F/K σ.σ., L αλγεβρική επέκταση του F και $E := \overline{K}^L$, τότε το L/E είναι *επέκταση* του F/K (συμβ. $F \le L$). Αν $[L : F] < \infty$, τότε η $F \le L$ είναι *πεπερασμένη επέκταση*.

Ο παραπάνω ορισμός είναι καλός και εμείς θα ασχοληθούμε μόνο με πεπερασμένες επεκτάσεις.

$$\begin{tikzcd}
& L \arrow[dl, dash, "\text{πεπερασμένη}"'] \arrow[dr, dash, "\text{υπερβατική βαθμού 1}"] & \\
F \arrow[dr, dash, "\text{υπερβατική βαθμού 1}"'] & & E \arrow[dl, dash, "\text{πεπερασμένη}"] \\
& K &
\end{tikzcd}$$

Σχήμα: Το L/E είναι πεπερασμένη επέκταση του F/K.

Οι πρώτοι στις επεκτάσεις

Ορισμός

Έστω $P \in \mathbb{P}_F$ και $\mathfrak{P} \in \mathbb{P}_L$. Λέμε ότι ο $\mathfrak{P}$ *βρίσκεται πάνω* (lies above) από τον P (συμβ. $\mathfrak{P} \mid P$) αν $\mathcal{O}_P = \mathcal{O}_{\mathfrak{P}} \cap F$ και $P = \mathfrak{P} \cap \mathcal{O}_P$.

Πρόταση

Αν P και $\mathfrak{P}$ όπως πριν, τότε

1. *το $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ είναι $\mathcal{O}_P/P$-διανυσματικός χώρος πεπερασμένης διάστασης,*
2. *$P\mathcal{O}_{\mathfrak{P}} = \mathfrak{P}^e$ για κάποιον ακέραιο $e \geq 1$,*
3. *για κάθε $\mathfrak{P} \in \mathbb{P}_L$ υπάρχει μοναδικό $P \in \mathbb{P}_F$ με $\mathfrak{P} \mid P$ και*
4. *για κάθε $P \in \mathbb{P}_F$ υπάρχει τουλάχιστον ένα, αλλά πεπερασμένα το πλήθος στοιχεία του $\mathbb{P}_L$ που βρίσκονται πάνω από αυτό.*

Μεγέθη που χαρακτηρίζουν τις επεκτάσεις

Ορισμός

Αν $\mathfrak{P} \mid P$ ως *σχετικό βαθμό* (relative degree ή inertia degree) των $\mathfrak{P}$ και P ορίζουμε τον αριθμό $f(\mathfrak{P}/P) := \left[{}^{\mathcal{O}_{\mathfrak{P}}}/_{\mathfrak{P}} \ : \ {}^{\mathcal{O}_P}/_{P}\right]$ και ως *δείκτη διακλάδωσης* (ramification index) των $\mathfrak{P}$ και P (συμβ. $e(\mathfrak{P}/P)$) τον ακέραιο e εκείνο που $P\mathcal{O}_{\mathfrak{P}} = \mathfrak{P}^e$.

Θεώρημα (Θεμελιώδης Ταυτότητα)

Αν $P \in \mathbb{P}_F$, $\{\mathfrak{P}_1, \dots, \mathfrak{P}_m\} \subseteq \mathbb{P}_L$ οι πρώτοι του L/E που βρίσκονται πάνω από τον P, $e_i := e(\mathfrak{P}_i/P)$ και $f_i := f(\mathfrak{P}_i/P)$, τότε

$$\sum_{i=1}^{m} e_i f_i = [L : F].$$

Επεκτάσεις σταθερού σώματος

Ορισμός

Αν E αλγεβρική επέκταση του K και $L = EF$, τότε έχουμε μια *επέκταση σταθερού σώματος*.

- Το E είναι το σώμα σταθερών του EF.

Πρόταση

Το γένος, g, του F/K είναι ίσο με το γένος, g', του L/E.

Οι πρώτοι στις επεκτάσεις σταθερού σώματος

Λήμμα

Αν $P \in \mathbb{P}_F$, τότε οι πρώτοι του L/E που βρίσκονται πάνω από τον P αδρανούν.

Πρόταση

Έστω K τέλειο, $P \in \mathbb{P}_F$ και ${}^{\mathcal{O}_P}/_P = K[\theta]$. Αν $h(X) := \mathrm{Irr}(\theta, K)$ και

$$h(X) = h_1(X) \cdots h_m(X)$$

η ανάλυση του $h(X)$ σε ανάγωγα στο $E[X]$, τότε υπάρχουν ακριβώς m το πλήθος πρώτοι του L/E που βρίσκονται πάνω από τον P. Αν $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_m\}$ οι πρώτοι αυτοί, τότε (ενδεχομένως μετά από κάποια αναδιάταξη) για $i = 1, \ldots, m$ ισχύει ότι $\deg_L \mathfrak{P}_i = \deg h_i(X)$.

Σημείωση: Από εδώ και πέρα θα ασχολούμαστε με το ολικό σ.σ. $F/\mathbb{F}$ και επεκτάσεις του. Θεωρούμε ότι $q := |\mathbb{F}|$, $p := \operatorname{char} \mathbb{F}$ και g το γένος του $F/\mathbb{F}$.

Ορισμός

Θέτουμε $a_n := |\{P \in \mathbb{P}_F \mid \deg P = n\}|$ και $b_n := |\{A \in \mathcal{D}_F \mid \deg A = n \text{ και } A \geq 0\}|$.

- Ισχύει ότι $b_n < \infty$ για κάθε n.

Θεώρημα (F. K. Schmidt)

Ισχύει ότι $a_1 > 0$.

Η συνάρτηση ζήτα του Riemann

Ορισμός

Αν $NA := q^{\deg A}$, ορίζουμε τη συνάρτηση ζήτα ως

$$\zeta_F(s) := \sum_{A \in \mathcal{D}_F, A \geq 0} NA^{-s}, \quad s \in \mathbb{C}.$$

1. Γράφεται και με τη μορφή γινομένου Euler ως
$$\zeta_F(s) = \prod_{n=1}^{\infty} (1 - q^{-ns})^{-a_n}.$$
2. Αν $u := q^{-s}$ γράφεται ως δυναμοσειρά ως
$$Z_F(u) := \zeta_F(s) = \sum_{n=0}^{\infty} b_n u^n.$$
3. Όλες αυτές οι εκφράσεις συγκλίνουν απόλυτα για $\Re s > 1$.
4. Επεκτείνεται αναλυτικά στο $\mathbb{C}$ με απλούς πόλους στα σημεία $s = 0$ και $s = 1$.

Πρόταση

Υπάρχει κάποιο $L_F(u) \in \mathbb{Z}[u]$, με $\deg L_F = 2g$ τέτοιο ώστε

$$\zeta_F(s) = \frac{L_F(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

Ακόμα $L_F(0) = 1$, $L_F(1) \neq 0$ και $L'_F(0) = a_1 - 1 - q$.

Το πολυώνυμο L_F ονομάζεται *L-πολυώνυμο* του $F/\mathbb{F}$.

Θεώρημα (Συναρτησιακή Εξίσωση της ζ)

Για κάθε $s \in \mathbb{C}$ έχουμε ότι

$$q^{(g-1)(1-s)}\zeta_F(1-s) = q^{(g-1)s}\zeta_F(s).$$

Το θεώρημα Hasse-Weil

- Το θεώρημα Hasse-Weil είναι η υπόθεση Riemann για σ.σ..
- Διατυπώθηκε από τον Artin ως εικασία και αποδείχθηκε από τον Weil (1948).
- Οι αποδείξεις του Weil είναι πολύπλοκες, αλλά η απόδειξη του Bombieri (1973) είναι αρκετά πιο απλή. Μέρος αυτής της απόδειξης θα παρουσιάσουμε.

Θεώρημα (Hasse-Weil)

Όλες οι ρίζες της συνάρτησης ζήτα βρίσκονται πάνω στην ευθεία $\{s \in \mathbb{C} \mid \Re s = 1/2\}$.

- Τέλος, $L_F(u) = \prod_{j=1}^{2g}(1 - \rho_j u)$ και s ρίζα της ζ_F ανν q^{-s} ρίζα του L_F. Έτσι μια εναλλακτική διατύπωση του Hasse-Weil θα ήταν ότι $|\rho_j| = q^{1/2}$.

Θέτουμε $F_r := F \cdot \mathbb{F}_{q^r}$, οπότε το σ.σ. $F_r/\mathbb{F}_{q^r}$ είναι επέκταση σταθερού σώματος του $F/\mathbb{F}$. Ισχύουν τα παρακάτω λήμματα.

Λήμμα

Έστω $m \in \mathbb{Z}_{>0}$. Το θεώρημα Hasse-Weil ισχύει για το $F/\mathbb{F}$ ανν ισχύει για το $F_m/\mathbb{F}_{q^m}$.

Λήμμα

Αν υπάρχει κάποιο $c \in \mathbb{R}$ τέτοιο ώστε για κάθε $r \geq 1$ να ισχύει ότι

$$|a_{F_r,1} - (q^r + 1)| \leq cq^{r/2},$$

τότε ισχύει το θεώρημα Hasse-Weil για το $F/\mathbb{F}$.

Για κάθε $r \geq 1$ ισχύει ότι

$$L_{F_r}(u) = \prod_{i=1}^{2g}(1 - \rho_i^r u) \quad \Rightarrow \quad L'_{F_r}(0) = -\sum_{i=1}^{2g} \rho_i^r$$

$$\Rightarrow a_{F_r,1} - (q^r + 1) = -\sum_{i=1}^{2g} \rho_i^r \quad \Rightarrow \quad \left|\sum_{i=1}^{2g} \rho_i^r\right| \leq c q^{r/2}.$$

Θέτουμε $H(t) := \sum_{i=1}^{2g} \frac{\rho_i t}{1-\rho_i t}$ και $\mu := \min\{|\rho_i^{-1}| \mid 1 \leq i \leq 2g\}$ και η ακτίνα σύγκλισης της δυναμοσειράς της $H(t)$ είναι ακριβώς μ. Για $|t| < \mu$ έχουμε ότι

$$H(t) = \sum_{i=1}^{2g}\sum_{r=1}^{\infty}(\rho_i t)^r = \sum_{r=1}^{\infty}\left(\sum_{i=1}^{2g}\rho_i^r\right)t^r.$$

Όμως, η τελευταία δυναμοσειρά θα συγκλίνει για $|t| < q^{-1/2}$, άρα $q^{-1/2} \leq \mu$, δηλαδή $q^{1/2} \geq |\rho_i|$ για κάθε i. Τέλος, η συναρτησιακή εξίσωση της ζ δίνει ότι $\prod_{j=1}^{2g} \rho_j = q^g$, οπότε $|\rho_j| = q^{1/2}$ για κάθε j.

Πρόταση

Αν q τετράγωνο $> (g+1)^4$, τότε $a_1 - (q+1) < (2g+1)\sqrt{q}$.

Απόδειξη.

1. Έστω $Q \in \mathbb{P}_F$, με $\deg Q = 1$. Θέτουμε $m := \sqrt{q} - 1$, $n := 2g + \sqrt{q}$ και $r := m + n\sqrt{q}$. Θεωρούμε το χώρο $\mathcal{L} := \mathcal{L}(mQ)\mathcal{L}(nQ)^{\sqrt{q}}$, που αποτελείται από όλα τα αθροίσματα της μορφής $\sum x_\nu y_\nu^{\sqrt{q}}$, με $x_\nu \in \mathcal{L}(mQ)$ και $y_\nu \in \mathcal{L}(nQ)$, δηλαδή $\mathcal{L} \subseteq \mathcal{L}(rQ)$.
2. Αποδεικνύεται ότι υπάρχει κάποιο $x \in \mathcal{L}^*$ τέτοιο ώστε όλοι οι πρώτοι του $F/\mathbb{F}$ βαθμού 1, εκτός του Q, να είναι ρίζες του, άρα $(x)_0 \geq \sum_{P \in \mathbb{P}_F,\, \deg P = 1,\, P \neq Q} P$, δηλαδή $\deg(x)_0 \geq a_1 - 1$.
3. Ακόμα $(x)_\infty \leq rQ$, δηλαδή $\deg(x)_\infty \leq r$. Όμως $r = q - 1 + (2g+1)\sqrt{q}$ και $\deg(x)_0 = \deg(x)_\infty$. □

Πρόταση

Υπάρχουν σταθερές c_1, c_2, που εξαρτώνται αποκλειστικά από το $F/\mathbb{F}$, τέτοιες ώστε αν q τετράγωνο και $q > c_1$, τότε για κάθε $r \geq 1$

$$a_{F_r,1} - (q^r + 1) > c_2\sqrt{q^r}.$$

Η απόδειξη της πρότασης χρησιμοποιεί επεκτάσεις Galois που δεν μελετήσαμε.

1. Συνδυάζοντας τα δύο προηγούμενα φράγματα και το γεγονός ότι το γένος, στις επεκτάσεις σταθερού σώματος, μένει αναλλοίωτο, παίρνουμε ότι υπάρχουν s, c τέτοια ώστε για κάθε r, που είναι ακέραιο πολλαπλάσιο του s, ισχύει ότι

$$|a_{F_r,1} - (q^r + 1)| \leq cq^{r/2}.$$

2. Από το 2° λήμμα των προκαταρκτικών, αυτό συνεπάγεται ότι ισχύει το Hasse-Weil για το $F_s/\mathbb{F}_{q^s}$.
3. Από το 1° λήμμα των προκαταρκτικών, το τελευταίο μας αποδεικνύει το Hasse-Weil για το $F/\mathbb{F}$.

Το θεώρημα των πρώτων αριθμών

Θεώρημα (Πρώτων Αριθμών)

$$a_N = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

- Το κλασικό θεώρημα των πρώτων αριθμών είναι ασθενέστερο.
- Το αντίστοιχο στην κλασική Θεωρία Αριθμών είναι ισοδύναμο με την υπόθεση Riemann και είναι ανοιχτό.
- Στην απόδειξη χρησιμοποιούμε το θεώρημα Hasse-Weil, αλλά αποδεικνύεται και ένα ασθενέστερο αποτέλεσμα και χωρίς αυτό.

Ισχύει ότι $L_F(u) = \prod_{j=1}^{2g}(1-\rho_j u)$, άρα $\frac{\prod_{j=1}^{2g}(1-\rho_j u)}{(1-u)(1-qu)} = \prod_{d=1}^{\infty}(1-u^d)^{-a_d}$. Αυτό μετά από πράξεις δίνει ότι

$$\sum_{k=1}^{\infty} u^k + \sum_{k=1}^{\infty}(qu)^k - \sum_{j=1}^{2g}\sum_{k=1}^{\infty}(\rho_j u)^k = \sum_{d=1}^{\infty}\sum_{k=1}^{\infty} d a_d u^{dk},$$

δηλαδή $1 + q^N - \sum_{j=1}^{2g} \rho_j^N = \sum_{d|N} d a_d$ και από τον τύπο αντιστροφής Möbius

$$N a_N = \sum_{d|N} \mu(d) q^{N/d} + \sum_{d|N} \mu(d) \left(\sum_{j=1}^{2g} \rho_j^{N/d} \right).$$

Όμως $\sum_{d|N} \mu(d) q^{N/d} = q^N + O(q^{N/2})$ και από Hasse-Weil $|\rho_j| = q^{1/2}$, άρα $\sum_{d|N} \mu(d) \left(\sum_{j=1}^{2g} \rho_j^{N/d} \right) = O(q^{N/2})$.

Ενδεικτική βιβλιογραφία

- Bombieri Enrico, "Counting Points on Curves Over Finite Fields", *Séminaire Bourbaki, n° 430*, p. 234-241, 1973.
- Rosen Michael, *Number Theory in Function Fields*, Springer, New York, 2002.
- Schmidt Friedrich Karl, "Analytische Zahlentheorie in Körpern der Charakteristik p", *Mathematische Zeitschrift, vol. 33, n° 1*, p. 1–32, 1931.
- Stichtenoth Henning, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin Heidelberg, 1993.
- Weil André, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.

Σας Ευχαριστούμε!