תורת המספרים האלגברית (88798) תשפ"א
תרגיל 12

1. יהי $\mathcal{O}$ חוג הערכה בדידה עם אידאל מקסימלי $\mathfrak{p}$. יהי $f[x] \in \mathcal{O}[x]$ פולינום. הוכח שקיים פולינום $g \in \mathcal{O}[x,y]$ שמקיים

$$f(x+y) = f(x) + f'(x)y + g(x,y)y^2.$$

2. יהי $\mathcal{O}$ כמו בשאלה הקודמת, ויהי $f(x) \in \mathcal{O}[x]$. יהי $\alpha \in \mathcal{O}$ שורש של f, ונניח כי $f'(\alpha) \in \mathcal{O}^\times$. יהי β שורש של f כך ש־ $\alpha - \beta \in \mathfrak{p}$. הוכח כי $\alpha = \beta$.
רמז: הוכח באינדוקציה כי $\alpha - \beta \in \mathfrak{p}^n$ לכל $n \in \mathbb{N}$.

3. בשאלה הזאת נמצא את כל שורשי היחידה ב־ $\mathbb{Q}_p$.
   (א) יהיו $\alpha, \beta \in \mathbb{Q}_p$ שורשים פרימיטיביים n־י ו־ m־י בהתאמה. נניח כי $p \nmid nm$. הוכח שאם $\alpha \neq \beta$ אזי $\alpha \not\equiv \beta \bmod \mathfrak{p}$. הסק כי $n|(p-1)$.
   (ב) יהי $p > 2$ ראשוני, ויהי $1 \neq \zeta \in \mathbb{Z}_p$ איבר שמקיים $\zeta^p = 1$. הוכח כי $\zeta = 1 + p\eta$ עבור $\eta \in \mathbb{Z}_p$ וכי

$$0 = 1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} \equiv p + \frac{p(p-1)}{2} p\eta \bmod p^2\mathbb{Z}_p.$$

   הסק סתירה.
   (ג) יהי $\zeta \in \mathbb{Q}_2$ איבר שמקיים $\zeta^4 = 1$. הוכח כי $\zeta \in \{\pm 1\}$.
   (ד) יהי $\zeta \in \mathbb{Q}_p$ שורש של 1. הוכח כי $\zeta^{p-1} = 1$ אם $p > 2$ וכי $\zeta \in \{\pm 1\}$ אם $p = 2$.

4. בשאר השאלות של התרגיל, L/K תהיה הרחבת גלואה סופית, כאשר K הינו שדה הנזלי עם הערכה v בדידה ומנורמלת, כלומר $v(K^\times) = \mathbb{Z}$. תהיה w ההמשכה של v ל־ L. תהי $v_L = ew$ ההערכה המנורמלת של L השקולה ל־ w. לכל $s \geq -1$ ממשי נגדיר

$$G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : v_L(\sigma(\alpha) - \alpha) \geq s + 1 \, \forall \alpha \in \mathcal{O}_L\}.$$

   (א) הוכח כי $G_s(L/K) \trianglelefteq \mathrm{Gal}(L/K)$ לכל s.
   (ב) יהי $\pi_L \in \mathcal{O}_L$ מאחד. הוכח לכל $s \geq 0$ שלם שההעתקה

$$\begin{aligned} G_s(L/K)/G_{s+1}(L/K) &\to U_L^{(s)}/U_L^{(s+1)} \\ \sigma &\mapsto \sigma(\pi_L) \cdot \pi_L^{-1} \end{aligned}$$

   הינה מונומורפיזם של חבורות ואינה תלויה בבחירה של π_L. כאן $U_L^{(0)} = \mathcal{O}_L^\times$, ואילו $U_L^{(s)} = 1 + \mathfrak{p}_L^s$ לכל $s \in \mathbb{N}$.
   (ג) תהי $K \subseteq M \subseteq L$ תת־הרחבה. הוכח כי

$$G_s(L/M) = G_s(L/K) \cap \mathrm{Gal}(L/M)$$

   לכל $s \geq -1$.

(ד) לכל $n \in \mathbb{N} \cup \{0\}$ נומר שההרחבה L/K הינה n־הרחבה עם n הינו השלם האי־שלילי המינימלי שמקיים $G_n(L/K) = \{e\}$. הוכח כי L/K הינה 0־הרחבה אם ורק אם היא לא מסועפת ושהיא 1־הרחבה אם ורק אם היא מתונה ומסתעפת.

המושג של n־הרחבה לא מוצלח עבור $n \geq 2$ כי אז הקומפוזיטום של n־הרחבות אינו בהכרח n־הרחבה. הוכח את זה על ידי דוגמא. לכן אי אפשר לקבל כך שרשרת יורדת טבעית של תת־חבורות של $\mathrm{Gal}(\overline{K}/K)$.

5. לכל $n \in \mathbb{N}$ יהי $K_n = \mathbb{Q}_p(\zeta_{p^n})$, כאשר ζ_{p^n} הינו שורש p^n־ י פרימיטיבי של 1. הוכח כי

$$G_s(K_n/\mathbb{Q}_p) = \begin{cases} \mathrm{Gal}(K_n/\mathbb{Q}_p) & : s = 0 \\ \mathrm{Gal}(K_n/K_m) & : p^{m-1} \leq s \leq p^m - 1,\ 1 \leq m \leq n-1 \\ \{e\} & : s \geq p^{n-1}. \end{cases}$$

6. נניח בנוסף להנחנות של השאלה הרביעית כי ההרחבה ℓ/k של שדות השארית הינה ספרבילית. במקרה הזה, ידוע שקיים איבר $\alpha \in \mathcal{O}_L$ כך ש־ $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. נגדיר פונקציה $i_{L/K} : \mathrm{Gal}(L/K) \to \mathbb{Z}$ על ידי $i_{L/K}(\sigma) = v_L(\sigma(\alpha) - \alpha)$. הוכח כי $i_{L/K}$ לא תלויה בבחירה של α וכי $G_s(L/K) = \{\sigma \in \mathrm{Gal}(L/K) : i_{L/K}(\sigma) \geq s+1\}$.

7. נגדיר פונקציה $\eta_{L/K} : [-1,\infty) \to [-1,\infty)$ על ידי

$$\eta_{L/K}(s) = \int_0^x \frac{dx}{[G_0(L/K) : G_x(L/K)]} = \\ \frac{1}{|G_0(L/K)|}\left(|G_1(L/K) + \cdots + |G_m(L/K)| + (s-m)|G_{m+1}(L/K)|\right),$$

כאשר $m \leq s \leq m+1$ עבור $m \geq 0$ שלם.

הוכח כי

$$\eta_{L/K}(s) = \frac{1}{|G_0(L/K)|} \sum_{\sigma \in \mathrm{Gal}(L/K)} \min\{i_{L/K}(\sigma), s+1\} - 1.$$

8. תהי $K \subseteq M \subseteq L$ תת־הרחבה. נסמן $H = \mathrm{Gal}(L/M)$.

(א) יהי $\rho \in \mathrm{Gal}(M/K)$ ונבחר $\sigma \in \mathrm{Gal}(L/K)$ כך ש־ $\sigma_{|M} = \rho$ וכך ש־ $i_{L/K}(\sigma)$ מקסימלי בין כל האיברים המקיימים את התנאי הראשון. יהי $\tau \in H$. הוכח כי $i_{L/K}(\sigma\tau) = \min\{i_{L/K}(\tau), i_{L/K}(\sigma)\}$.

רמז: טפל בנפרד במקרה $\tau \in G_{i_{L/K}(\sigma)-1}(L/M)$ ובמקרה $\tau \notin G_{i_{L/K}(\sigma)-1}(L/M)$.

(ב) הוכח כי $|G_0(L/M)| = e(L/M)$.

(ג) ידוע כי $i_{M/K}(\tau) = \frac{1}{e(L/M)} \sum_{\substack{\sigma \in \mathrm{Gal}(L/K) \\ \sigma_{|M} = \tau}} i_{L/K}(\sigma)$ לכל $\tau \in \mathrm{Gal}(M/K)$.

אפשר למצוא הוכחה של העובדה הזאת, כמו של כל סדרת התרגילים הזאת, בפרק 10 של החלק השני של נויקירך. היעזר בעובדה הזאת והוכח כי $i_{M/K}(\rho) - 1 = \eta_{L/M}(i_{L/K}(\sigma) - 1)$.

(ד) הוכח כי

$$G_s(L/K)H/H = G_{\eta_{L/M}(s)}(M/K)$$

לכל $s \geq -1$.

9. הוכח שהפונקציה $\eta_{L/K}$ חד־חד־ערכית. לכן יש לה פונקציה הפכית, נסמן אותה $\psi_{L/K}$. לכל תת־הרחבה $K \subseteq M \subseteq L$, הוכח כי $\eta_{L/K} = \eta_{M/K} \circ \eta_{L/M}$ ולכן כי $\psi_{L/K} = \psi_{L/M} \circ \psi_{M/K}$.

10. לכל הרחבה L/K המקיימת את התנאים שלנו, נגדיר

$$G^t(L/K) = G_{\psi_{L/K}(t)}(L/K)$$

לכל $t \geq -1$. יהיו M, H כמו למעלה. הוכח כי

$$G^t(L/K)H/H = G^t(M/K).$$

11. הוכח שניתן להגדיר

$$G^t(\overline{K}/K) = \varprojlim_{[L:K]<\infty} G^t(L/K) \leq \mathrm{Gal}(\overline{K}/K).$$

הוכח שאם נגדיר הרחבה L/K הינה n־ מסועפת כמו בסעיף האחרון של השאלה הרביעית, אבל עם חבורות ההסתעפות העליונות $G^n(L/K)$ במקום התחתונות. הוכח שיש הרחבה n־ מסועפת מקסימלית K^n/K וכי $G^n(\overline{K}/K) = \mathrm{Gal}(\overline{K}/K^n)$.