תורת המספרים האלגברית (88798) תשפ"א
תרגיל 6

1. יהי $n = p^a$ כאשר p ראשוני, יהי ζ_n שורש n־י פרימיטיבי של 1, ויהי $L_n = \mathbb{Q}(\zeta_n)$ שדה ציקלוטימי. יהי $\pi = 1 - \zeta_n$.
   (א) הוכח כי $\mathcal{O}_{L_n}/(\pi) \simeq \mathbb{F}_p$.
   (ב) הוכח כי $\mathcal{O}_{L_n} = \mathbb{Z}[\zeta_n] + \pi\mathcal{O}_{L_n}$ כחבורות אבליות.
   (ג) הוכח, בעזרת הסעיף הקודם, כי $\mathcal{O}_{L_n} = \mathbb{Z}[\zeta_n] + \pi^2\mathcal{O}_{L_n}$ כחבורות אבליות.
   (ד) הוכח כי $\mathcal{O}_{L_n} = \mathbb{Z}[\zeta_n]$.
2. יהי $n = p^a$ כמו בשאלה הקודמת.
   (א) יהי $\Phi_n(x)$ הפולינום המינימלי של ζ_n ותהי $\Phi'_n(x)$ הנגזרת שלו. הוכח כי $d_{\mathbb{Q}(\zeta_n)} = \pm N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\Phi'_n(\zeta_n))$. רמז: וונדרמונד.
   (ב) הוכח כי $\Phi'_n(\zeta) = \frac{p^a\zeta^{p^a-1}}{\zeta^{p^{a-1}}-1}$.
   (ג) הוכח כי $d_{\mathbb{Q}(\zeta_n)} = \pm p^{p^{a-1}(ap-a-1)}$.
3. הוכח שלא קיים שדה מספרים K כך ש־ $d_K = \pm 1$.
4. יהיו K, L שדות מספרים. נניח כי $(d_K, d_L) = 1$.
   (א) הוכח כי $K \cap L = \mathbb{Q}$.
   (ב) הוכח כי $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$.
5. יהי A תחום ראשי. בפרט, הוא תחום דדקינד. יהי $K = \operatorname{Frac} A$, ותהיינה L, L' שתי הרחבות ספרביליות של K שמקיימות $L \cap L' = K$. יהיו B, B' הסגורות השלמים של A ב־ L, L' בהתאמה, ויהיו $\{\beta_1, \dots, \beta_n\}$ בסיס שלם של B ו־ $\{\beta'_1, \dots, \beta'_m\}$ בסיס שלם של B'. נניח כי הדיסקרימיננטות $d_{L/K}, d_{L'/K}$ זרות בתור אידאלים של A.
   (א) הוכח כי $\{\beta_i\beta'_j : 1 \le i \le n, 1 \le j \le m\}$ הינו בסיס של LL' מעל K.
   (ב) יהי $\mathcal{O}$ הסגור השלם של A ב־ LL'. יהי $x \in \mathcal{O}$ ויהי $x = \sum_{i,j} a_{ij}\beta_i\beta'_j$, כאשר $a_{ij} \in K$. הגדר $b_j = \sum_{i=1}^n a_{ij}\beta_i$ לכל $1 \le j \le m$. הוכח כי $b_j d_{L'/K} \subset B$ לכל j ולכן כי $a_{ij}d_{L'/K}$ הינו אידאל שלם של A לכל זוג i, j.
   (ג) הוכח באופן דומה כי $a_{ij}d_{L/K}$ הינו אידאל שלם של A לכל זוג i, j.
   (ד) הסק כי $\{\beta_i\beta'_j : 1 \le i \le n, 1 \le j \le m\}$ הינו בסיס שלם של $\mathcal{O}$.
   (ה) הוכח כי $d_{LL'/K} = (d_{L/K})^m(d_{L'/K})^n$.
6. הוכח כי $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ לכל n טבעי.
7. תהי L/K הרחבת גלואה של שדות מספרים. נניח כי $\operatorname{Gal}(L/K)$ לא ציקלית. הוכח שאם אידאל ראשוני $\mathfrak{p}$ לא מתפצל ב־ L, אזי הוא מסתעף. בפרט, יש מספר סופי של אידאלים כאלה.

8. תהי G חבורה ותהיינה $U,V \leq G$ שתי תת־חבורות. יהיו $g,h \in G$. נגיד כי $g \sim h$ אם קיימים $u \in U, v \in V$ כך ש־ $h = ugv$. הוכח שזה יחס שקילות. מחלקות השקילות נקראות מחלקות כפולות, או קוסטים כפולים, ואת הקבוצה של המחלקות הכפולות מסמנים $U\backslash G/V$.

9. יהיו A,B,K,L כרגיל ויהי N הסגור הנורמלי של L מעל K. כלומר, N/K הינה הרחבת גלואה המינימלית המקיימת $L \subseteq N$. יהי C הסגור השלם של A ב־ N. תהי $G = \mathrm{Gal}(N/K)$ ותהי $H = \mathrm{Gal}(N/L) \leq G$. יהי $\mathfrak{p}$ אידאל ראשוני לא־אפסי של A ויהי Q אידאל ראשוני של C כך ש־ $Q|\mathfrak{p}$. תהי $G_Q \leq G$ תת־חבורת הפירוק. תהי $\mathcal{S}_\mathfrak{p}$ הקבוצה של כל האידאלים הראשוניים של B שמחלקים $\mathfrak{p}$.

(א) נגדיר העתקה $\psi : H\backslash G/G_Q \to \mathcal{S}_\mathfrak{p}$ על ידי $\psi(H\sigma G_Q) = \sigma(Q) \cap B$ מוגדרת היטב וכי היא חד־חד־ערכית ועל.

(ב) נניח כי $\mathfrak{p}$ מתפצל לגמרי ב־ L. הוכח כי $H\sigma G_Q = H\sigma$ לכל $\sigma \in G$ ולכן כי $\sigma G_Q \subseteq \sigma H$.

(ג) יהי $\tilde{H} = \bigcap_{\sigma \in G} \sigma^{-1} H \sigma$. הוכח כי $\tilde{H} \trianglelefteq H$ תת־חבורה נורמלית וכי $G_Q \leq \tilde{H}$.

(ד) הוכח כי $\tilde{H} = H$ או $\tilde{H} = \{e\}$ ובשני המקרים הוכח כי $\mathfrak{p}$ מתפצל לגמרי ב־ N.

(ה) הוכח את הטענה השימושית הבאה: $\mathfrak{p}$ מתפצל לגמרי ב־ L ואם ורק אם הוא מתפצל לגמרי ב־ N.