ב"ה

תורת המספרים האלגברית (88-798)

קובץ 5

1.) יהי $\{a_n\}$ סדרת קושי של איברים $a_i \in K$ שמתכנסת לאיזה $x \in K_\wp$.
צריך להראות שאם נסתכל על ה-a_i כאיברים של L, אז $\{a_n\}$ עדיין סדרת קושי ביחס לערך המוחלט $|\cdot|_P$.

יהי $e = e(P|\wp)$ אינדקס ההסתעפות. זה אומר ש-$P^e | \wp O_L$ $\Rightarrow$ בפרט, $\wp O_L \subseteq P^e$.

$v_\wp(a_n - a_m) \ge n \Rightarrow a_n - a_m \in \wp^n \Rightarrow a_n - a_m \in \wp^n O_L$ (כאיברים של L) $\Rightarrow a_n - a_m \in P^{ne} \Rightarrow v_P(a_n - a_m) \ge ne$.

$\{a_n\}$ היא סדרת קושי ביחס ל-$|\cdot|_P$ אם ורק אם לכל $\varepsilon > 0$ קיים N כך ש-$m,n \ge N \Rightarrow v_P(a_n - a_m) \ge -\log \varepsilon$. כיוון ש-$\{a_n\}$ היא סדרת קושי ביחס ל-$|\cdot|_\wp$, קיים N כך ש-$m,n \ge N \Rightarrow v_\wp(a_n - a_m) \ge -\log \varepsilon$. אך זה אומר $(v_P(a_n - a_m) \ge -e\log\varepsilon \ge -\log \varepsilon)$.
ברור שהשיכון הזה מוגדר היטב ושהוא אכן שיכון שדות.

2.) ברור ש-$(\mathbb{Z}_p^*)^2$ (כל האיברים של $\mathbb{Z}_p^*$ שהם ריבועים) היא תת-חבורה של $\mathbb{Z}_p^*$. אנחנו טוענים שיש לה אינדקס 2. נשתמש באיזומורפיזם $\varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$, ונראה איבר $x \in \mathbb{Z}_p$ כסדרה $x = (a_1, a_2, \dots)$, כאשר

$a_n \in \mathbb{Z}/p^n\mathbb{Z}$ ו-$a_n = \varphi_{m,n}(a_m)$ עבור $m \ge n$ $(\varphi_{m,n} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z})$.

ברור ש-$x \notin \mathbb{Z}_p^* \iff x \in p\mathbb{Z}_p \iff a_1 = 0 \iff a_n \equiv 0 \pmod{p}$ עבור איזשהו $n \in \mathbb{N}$. לכן, $\cancel{x\notin}$ $x \in \mathbb{Z}_p^* \iff a_n \not\equiv 0 \pmod{p}$ לכל n.

עכשיו, $a_n \not\equiv 0\ (p) \iff a_n \notin p \cdot \mathbb{Z}/p^n\mathbb{Z} \iff a_n \in (\mathbb{Z}/p^n\mathbb{Z})^*$.

אבל $|(\mathbb{Z}/p^n\mathbb{Z})^*| = p^{n-1}(p-1)$, וכיוון שקיימת העתקה על $(\mathbb{Z}/p^n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$

אנחנו רואים ש- $(\mathbb{Z}/p^n\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times P$, כאשר P היא חבורה כך שהסדר שלה הינו חזקה של p. ברור ש- $((\mathbb{Z}/p^n\mathbb{Z})^*)^2 \simeq (\mathbb{Z}/(p-1)\mathbb{Z})^2 \times P^2$.

המנה P/P^2 היא חבורה עם מעריך 2, לכן $|P/P^2| = 2^k$. אך $2 \nmid |P|$, כיוון ש- $(p \neq 2)$, לכן $|P/P^2|=1 \Rightarrow P=P^2$. ברור ש- $(\mathbb{Z}/(p-1)\mathbb{Z})^2 = 2\mathbb{Z}/(p-1)\mathbb{Z}$, ו- $(p-1)$ זוגי! לכן $((\mathbb{Z}/p^n\mathbb{Z})^*)^2$ היא תת-חבורה של $(\mathbb{Z}/p^n\mathbb{Z})^*$ של אינדקס 2, ולכן $(\mathbb{Z}_p^*)^2 \leq \mathbb{Z}_p^*$ תת-חבורה של אינדקס 2.

תהי $K/\mathbb{Q}_p$ הרחבה ריבועית. אזי $K=\mathbb{Q}_p(\sqrt{\alpha})$ עבור $\alpha\in\mathbb{Q}_p$ מתאים. כיוון ש- $K=\mathbb{Q}_p(\sqrt{\alpha})=\mathbb{Q}_p(p\sqrt{\alpha})=\mathbb{Q}_p(\sqrt{\alpha p^2})$, אפשר להכפיל את α בחזקה מתאימה (חיובית או שלילית) של p^2 ולהניח בלי הגבלת הכלליות כי $v_p(\alpha)\in\{0,1\}$.

אם $v_p(\alpha)=0$, אזי $\alpha\in\mathbb{Z}_p^*$. ברור ש- $\alpha\notin(\mathbb{Z}_p^*)^2$, כי אחרת $\mathbb{Q}_p(\sqrt{\alpha})=\mathbb{Q}_p$. מסתכלים בתמונות של α ו- u במנה $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \simeq \mathbb{Z}/2\mathbb{Z}$ ורואים ש- $\alpha u^{-1}\in(\mathbb{Z}_p^*)^2$. יהי $\alpha u^{-1}=x^2$. אזי $K=\mathbb{Q}_p(\sqrt{\alpha})=\mathbb{Q}_p(\sqrt{\alpha u^{-1}\cdot u})=\mathbb{Q}_p(\sqrt{x^2u})=\mathbb{Q}_p(x\sqrt{u})=\mathbb{Q}_p(\sqrt{u})$.

במקרה ש- $v_p(\alpha)=1$, נרשום $\alpha=py$ עבור $y\in\mathbb{Z}_p^*$. אם $y=x^2\in(\mathbb{Z}_p^*)^2$ אזי $K=\mathbb{Q}_p(\sqrt{\alpha})=\mathbb{Q}_p(\sqrt{px^2})=\mathbb{Q}_p(x\sqrt{p})=\mathbb{Q}_p(\sqrt{p})$. אחרת, $yu^{-1}=x^2\in(\mathbb{Z}_p^*)^2$, ולכן $K=\mathbb{Q}_p(\sqrt{\alpha})=\mathbb{Q}_p(\sqrt{p\cdot yu^{-1}\cdot u})=\mathbb{Q}_p(\sqrt{px^2u})=\mathbb{Q}_p(x\sqrt{pu})=\mathbb{Q}_p(\sqrt{pu})$.

3) יהיו $x,y\in K$ כך ש- $|x|\neq|y|$. ונניח בלי הגבלת הכלליות, כי $|x|>|y|$. כיוון שהערך המוחלט לא ארכימדי, מתקיים $|x+y|\le\max\{|x|,|y|\}=|x|$. אבל $x=(x+y)+(-y)$, ולכן $|x|\le\max\{|x+y|,|-y|\}=\max\{|x+y|,|y|\}$.

אך אנחנו יודעים ש- $|x|>|y|$, לכן חייב להתקיים $|x|\le|x+y|$. כבר הוכחנו את האי-שוויון ההפוך, לכן $|x+y|=|x|=\max\{|x|,|y|\}$.

4) נזכור ש- $\mathbb{Z}_p$ הוא $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. איבר $x=(a_1,a_2,\dots)\in\mathbb{Z}_p$ ($a_n\in\mathbb{Z}/p^n\mathbb{Z}$) מקיים $x^{p-1}=1$ אם ורק אם $a_n^{p-1}=1$ לכל n, כי ברור שהיחידה של $\mathbb{Z}_p$ הינה $(1,1,1,\dots)$.
איבר $a_n\in\mathbb{Z}/p^n\mathbb{Z}$ הפיך אם ורק אם $a_n\notin p\cdot\mathbb{Z}/p^n\mathbb{Z}$. כלומר,
$|(\mathbb{Z}/p^n\mathbb{Z})^*|=p^{n-1}(p-1)$. בפרט, אם קיים $a\in(\mathbb{Z}/p^n\mathbb{Z})^*$ כך ש- $a_n=a^{p^{n-1}}$, אזי $a_n^{p-1}=a^{p^{n-1}(p-1)}=1$ (כי כל איבר בחזקת סדר החבורה הוא 1).

נבחין גם בכך ש- $\varphi_{m,n}(a^{p^{m-1}}+p^m\mathbb{Z})=a^{p^{n-1}}+p^n\mathbb{Z}$. אכן, לפי אינדוקציה מספיק להוכיח את זה עבור $m=n+1$. אך $a^{p^n}=(a^{p^{n-1}})^p$ ו- $(a^{p^{n-1}})^{p^{n-1}}\cdot a^{p^{n-1}}=a^{p^{n-1}}$ ב- $\mathbb{Z}/p^n\mathbb{Z}$, כי כבר ראינו ש-($(a^{p^{n-1}})^{p^{n-1}}=1$). אזי, לכל $1\le a\le p-1$, הסדרה $(a+p\mathbb{Z}, a^p+p^2\mathbb{Z}, a^{p^2}+p^3\mathbb{Z},\dots)$ נותנת איבר מוגדר היטב של $\varprojlim\mathbb{Z}/p^n\mathbb{Z}$, והאיבר הזה הוא שורש $(p-1)$ של יחידה. לכן, $[\lambda]=(\lambda+p\mathbb{Z}, \lambda^p+p^2\mathbb{Z}, \lambda^{p^2}+p^3\mathbb{Z},\dots)$, וברור שאותה הנוסחה עובדת גם עבור $\lambda=0$.

6) יהיו $\lambda_0,\lambda_1\in\mathbb{F}_p$. אזי $[\lambda_0]+p[\lambda_1]+1=$

$$(\lambda_0+p\mathbb{Z}, \lambda_0^p+p^2\mathbb{Z},\dots)+(p\lambda_1+p\mathbb{Z}, p\lambda_1^p+p^2\mathbb{Z}, p\lambda_1^{p^2}+p^3\mathbb{Z},\dots)+$$
$$(1+p\mathbb{Z}, 1+p^2\mathbb{Z}, 1+p^3\mathbb{Z},\dots)=$$
$$(\lambda_0+1+p\mathbb{Z}, \lambda_0^p+p\lambda_1^p+1+p^2\mathbb{Z}, \lambda_0^{p^2}+p\lambda_1^{p^2}+1+p^3\mathbb{Z},\dots).$$

מאידך, $[\lambda_0+1] = (\lambda_0+1+p\mathbb{Z},\ (\lambda_0+1)^p + p^2\mathbb{Z},\ (\lambda_0+1)^{p^2}+p^3\mathbb{Z}, \dots)$

ולכן, $[\lambda_0]+p[\lambda_1]+1-[\lambda_0+1] =$

$$(*)\qquad (p\mathbb{Z},\ \lambda_0^p+1-(\lambda_0+1)^p + p\lambda_1^p + p^2\mathbb{Z},\ \dots)$$

עכשיו, נבחין כבר ש- $\lambda_0^p+1-(\lambda_0+1)^p$ מתחלק ב-p לפי המשפט הקטן של פרמה, וש-

$$p\left[\lambda_1 + \frac{\lambda_0^p+1-(\lambda_0+1)^p}{p}\right] =$$

$$\left(p\mathbb{Z},\ p\left(\lambda_1^p + \frac{\lambda_0^p+1-(\lambda_0+1)^p}{p}\right)^p + p^2\mathbb{Z}, \dots\right)$$

$= p\left(\lambda_1 + \frac{\lambda_0^p+1-(\lambda_0+1)^p}{p}\right)^p + p^2\mathbb{Z}$ ולכן, לכל $a\in\mathbb{Z}$, $a^p\equiv a \pmod p$ אך

$$p\left(\lambda_1^p + \frac{\lambda_0^p+1-(\lambda_0+1)^p}{p}\right) + \overset{p^2\mathbb{Z}}{=} p\left(\lambda_1 + \frac{\lambda_0^p+1-(\lambda_0+1)^p}{p}\right) + p.$$

אז רואים מן המשוואה (*) למעלה כי

$$[\lambda_0]+p[\lambda_1]+1 = [\lambda_0+1] + p\left[\lambda_1 + \frac{\lambda_0^p+1-(\lambda_0+1)^p}{p}\right] + \underbrace{(p\mathbb{Z},\ p^2\mathbb{Z}, \dots)}_{x}.$$

כיוון ש- $x\in p^2\mathbb{Z}_p$. כי הרי התמונה של x ב- $\mathbb{Z}_p/p^2\mathbb{Z}_p \cong \mathbb{Z}/p^2\mathbb{Z}$ היא 0, קיבלנו את החפיפה הנדרשת.