אנליזה הרמונית ושדות מספרים

אלעד זלינגר

תקציר

רשימות אלו מבוססות על ההרצאות בקורס "אנליזה הרמונית ושדות מספרים" (סימול 0366-5029) שהועבר על ידי פרופסור אשר בן־ארצי בסמסטר א' שנת הלימודים תשע"ו באוניברסיטת תל אביב. אין המרצה אחראי לכל טעות שנפלה ברשימות אלה. לתגובות, תיקונים ועוד, אנא פנו לelad88 בgmail.

תוכן עניינים

1 פונקציית Γ

1.1 הכנה

תזכורת על Fubini: יהיו (X, Σ_X, μ), (Y, Σ_Y, λ) שני מרחבי מידה σ־סופיים ו־$f : X \to Y$ מדידה לפי $\Sigma_X \times \Sigma_Y$.

1. אם $0 \leq f \leq \infty$ מתקיים

$$\begin{aligned}\int_X \left(\int_Y f(x,y)\, d\lambda(y)\right) d\mu(x) &= \int_{X\times Y} f(x,y)\, d(\mu\times\lambda)(x,y)\\ &= \int_Y \left(\int_X f(x,y)\, d\mu(x)\right) d\lambda(y)\end{aligned}$$

(ראה גם Rudin - Real/Complex analysis chapter 7)

2. אם f מרוכבת אז

$$\begin{aligned}\int_X \left(\int_Y |f(x,y)|\, d\lambda(y)\right) d\mu(x) &= \int_{X\times Y} |f(x,y)|\, d(\mu\times\lambda)(x,y)\\ &= \int_Y \left(\int_X |f(x,y)|\, d\mu(x)\right) d\lambda(y)\end{aligned}$$

אם מספר זה סופי, פרט לקבוצה מדידה ממידה 0 בX מתקיים

$$\int_Y |f(x,y)|\, d\lambda(y) \quad < \quad \infty$$

ומוגדר $\int_Y f(x,y)\, d\lambda(y) \in \mathbb{C}$ ומתקיים שוב

$$\begin{aligned} \int_X \left(\int_Y |f(x,y)|\, d\lambda(y) \right) d\mu(x) \quad &= \quad \int_{X\times Y} |f(x,y)|\, d(\mu\times\lambda)(x,y) \\ &= \quad \int_Y \left(\int_X |f(x,y)|\, d\mu(x) \right) d\lambda(y) \end{aligned}$$

לאחר שנותנים ערך $\int_Y f(x,y)\, d\lambda(y) = 0$ לאותם xים עבורם $\int_Y |f(x,y)|\, d\lambda(y) = \infty$ (וכנ"ל f אינטגרבילית בצד השני).

תזכורת על מכפלות:

1. אם $a_n \in \mathbb{C}$ עם $a_n \neq -1$ לכל n ומתקיים $\sum_{n=1}^{\infty} |a_n| < \infty$ אז קיים

$$\prod_{n=1}^{\infty} (1+a_n) \quad = \quad \lim_{N\to\infty} \prod_{n=1}^{N} (1+a_n) \in \mathbb{C}^*$$

וערכו אינו תלוי בסדר המכפלה. הסבר: די לבדוק שקיים $\sum_{n=1}^{\infty} \log(1+a_n)$, ומשתמשים בכך ש$\log(1+a_n) \approx a_n$.

2. אם f_n הולומורפית בתחום $G \subseteq \mathbb{C}$ לכל n טבעי ו$f_n(z) \neq -1$ לכל $z \in G$, וקיימים $M_n > 0$ כך ש$\sum_{n=1}^{\infty} M_n < \infty$ וכך ש$|f_n| < M_n$ על G אז

$$f(z) \quad = \quad \prod_{m=1}^{\infty} (1+f_m(z))$$

הולומורפית על G ולא מתאפסת בG.

הערה 1.1 יש קבועים $k_1, k_2 > 0$ כך שלכל $|z| < \frac{1}{2}$ מתקיים $k_1 \cdot |z| \leq |\log(1+z)| \leq k_2 \cdot |z|$. לכן אם $|f_n| \leq \frac{1}{2}$ בG, אז די לבדוק ש$|\log(1+f_n)| \leq M_n$.

3. **דוגמה:** נסמן פונקציה שלמה $\varphi(z) = (1+z)e^{-z} - 1$. פיתוח טיילור סביב 0:

$$\varphi(z) \quad = \quad (1+z)\left(1 - z + \frac{z^2}{2} - \dots\right) - 1 = -\frac{z^2}{2} + \dots$$

לכן קיים $k > 0$ כך ש $|\varphi(z)| \leq k|z|^2$ ל$|z| \leq 1$. לכן אם נגדיר f_n לפי $f_n(z) = \left(1+\frac{z}{n}\right)e^{-\frac{z}{n}} - 1$, אז מתקיים $f_n(z) = \varphi\left(\frac{z}{n}\right)$ ולכל $R > 0$ נתון מתקיים

$$|f_n(z)| \leq k \cdot \left|\frac{z}{n}\right|^2 \leq \frac{k\cdot R^2}{n^2} \qquad (|z| \leq R < n)$$

נייישם את 2 עם $M_n = \frac{k\cdot R^2}{n^2}$.

מסקנה 1.2 הפונקציה

$$F(z) = \prod_{n=1}^{\infty}(1+f_n(z)) = \prod_{n=1}^{\infty}\left(\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right)$$

היא פונקציה שלמה ומתאפסת רק בנקודות $z=-1,-2,-3,\ldots$. מכאן יש לה אפסים פשוטים.

הוכחה: עבור R נתון נקח n_0 עם $\frac{kR^2}{n_0^2}<1$. נכתוב

$$\prod_{n=1}^{\infty}\left(\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right) = \prod_{n=1}^{n_0}\left(\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right)\cdot\prod_{n=n_0+1}^{\infty}\left(\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right)$$

אז המכפלה השנייה מקיימת את תנאי המשפט ולכן הולומורפית ללא אפסים בתחום $|z|<R$. מדובר במכפלה של שתי פונקציות הולומורפיות ולכן הולומורפית. ■

1.2 פונקציית Γ

חלק זה מבוסס על Special Functions: A Graduate Text (Cambridge Studies in Advanced Mathematics) מאת Beals וWong.

הערה 1.3 אם $t>0$ ו$w\in\mathbb{C}$ אז מתקיים $t^w=e^{w\log t}$, ולכן $|t^w|=e^{\mathrm{Re}(w)\cdot\log t}=t^{\mathrm{Re}(w)}$.

הגדרה 1.4 עבור $\mathrm{Re}(z)>0$ נגדיר $\Gamma(z)=\int_0^\infty t^{z-1}e^{-t}dt$

1.3 תכונות

1. הולומורפיות: יהי $0<\varepsilon<1$. עבור $\varepsilon<\mathrm{Re}(z)<\frac{1}{\varepsilon}$ מתקיים

$$\left|t^{z-1}e^{-t}\right| \le \begin{cases} t^{\varepsilon-1}e^{-t} & (0\le t\le 1)\\ t^{\frac{1}{\varepsilon}-1}e^{-t} & (1\le t<\infty)\end{cases}$$

זה מראה הולומורפיות כי $\frac{\Gamma(z+h)-\Gamma(z)}{h}=\int_0^\infty\frac{t^{z+h-1}-t^{z-1}}{h}e^{-t}dt$ ולכן $\left|\frac{t^{z+h-1}e^{-t}-t^{z-1}e^{-t}}{h}\right|=\left|t^{z-1}e^{-t}\right|\left|\frac{t^h-1}{h}\right|$ ומאי־השוויון הנ"ל נובע כי $\int_0^\infty\left|\frac{t^{z+h-1}e^{-t}-t^{z-1}e^{-t}}{h}\right|dt<\infty$ ולכן ניתן להחליף גבול ואינטגרל ולקבל

$$\begin{aligned}\lim_{h\to0}\frac{\Gamma(z+h)-\Gamma(z)}{h} &= \lim_{h\to0}\int_0^\infty\frac{t^{z+h-1}-t^{z-1}}{h}e^{-t}dt\\ &= \int_0^\infty\lim_{h\to0}\frac{t^{z+h-1}-t^{z-1}}{h}e^{-t}dt\\ &= \int_0^\infty t^{z-1}e^{-t}\log t\,dt\end{aligned}$$

2. $\Gamma(1)=\int_0^\infty e^{-t}dt=-e^{-t}\mid_0^\infty=1$

3. משוואה פונקציונלית:

$$\Gamma(z+1)=z\Gamma(z)\qquad(\mathrm{Re}z>0)$$

הוכחה:

$$\begin{aligned}\Gamma(z+1) &= \lim_{\varepsilon\to0}\int_\varepsilon^{\frac{1}{\varepsilon}} t^z e^{-t}dt\\ &= \lim_{\varepsilon\to0}\int_\varepsilon^{\frac{1}{\varepsilon}} t^z\left(-e^{-t}\right)'dt\\ &= \lim_{\varepsilon\to0}\left[-t^z e^{-t}\mid_\varepsilon^{\frac{1}{\varepsilon}}-\int_\varepsilon^{\frac{1}{\varepsilon}}\left(t^z\right)'\left(-e^{-t}\right)dt\right]\\ &= \lim_{\varepsilon\to0}\left[-t^z e^{-t}\mid_\varepsilon^{\frac{1}{\varepsilon}}+\int_\varepsilon^{\frac{1}{\varepsilon}} zt^{z-1}e^{-t}dt\right]\\ &= z\int_0^\infty t^{z-1}e^{-t}dt=z\Gamma(z)\end{aligned}$$

■

מסקנה 1.5

1. $\Gamma(z+n)=\Gamma(z)\cdot z\cdot(z+1)\cdot\ldots\cdot(z+n-1)$ כאשר $n=1,2\ldots$

2. $\Gamma(n+1)=n!$ כאשר $n=0,1,2,\ldots$

3. המשכה מרומורפית: לכל $n=1,2,\ldots$ נגדיר ל-$\mathrm{Re}(z)>-n$ ו- $z\neq0,-1,\ldots-(n-1)$

$$\Gamma_n(z)=\frac{\Gamma(z+n)}{z(z+1)\cdot\ldots\cdot(z+n-1)}$$

אז Γ_n מרומורפית על $\mathrm{Re}(z)>-n$ ו-$\Gamma_n=\Gamma$ על $\mathrm{Re}(z)>0$. לכן $\Gamma_n=\Gamma_m$, לכל $m,n\geq1$ על תחום ההגדרה המשותף.

מסקנה 1.6 ל-Γ יש המשכה מרומורפית על כל המישור המרוכב עם לכל היותר קטבים פשוטים בנקודות $z=0,-1,-2,\ldots$.

הערה 1.7 המשוואה $\Gamma(z+1)=z\Gamma(z)$ ממשיכה להתקיים על המישור המרוכב.

4. הקטבים: $z=-n$ הוא קוטב פשוט של Γ עם שארית $\frac{(-1)^n}{n!}$ (כאן $n=0,1,2,\ldots$) ואלה כל הקטבים.

הוכחה: ראינו כי $\Gamma(1)=1$ ולכן $\Gamma(u+1)=1+a_1u+\ldots$ וגם

$$\Gamma(u+1) = \Gamma(u-n)\cdot(u-n)(u-(n-1))\cdot\ldots\cdot u$$

לכן

$$\begin{aligned}\Gamma(-n+u) &= \frac{\Gamma(u+1)}{u(u-1)\cdot\ldots\cdot(u-n)}\\ &= \frac{1}{u}\cdot\frac{(1+a_1u+\ldots)}{(u-1)\cdot\ldots\cdot(u-n)}\\ &= \frac{1}{u}\left(\frac{(-1)^n}{n!}+c_1u+\ldots\right)\end{aligned}$$

■

5. נוסחת המכפלה של אוילר: אם $\mathbb{C}\ni z\neq 0,-1,-2,\ldots$ אז

$$\lim_{n\to\infty}\frac{(n-1)!\cdot n^z}{z(z+1)\ldots(z+n-1)} = \Gamma(z)$$

נוכיח ראשית טענת עזר:

טענה 1.8 ל$0\le t\le n$ מתקיים

$$0\le e^{-t}-\left(1-\frac{t}{n}\right)^n \le \frac{e}{2}\cdot\frac{t^2e^{-t}}{n}$$

הוכחה: נסמן $f(x)=e^{-x}-(1-x)=e^{-x}-1+x$. אז $f'(x)=-e^{-x}+1$ ו$f''(x)=e^{-x}$ כאשר $x\in\mathbb{R}$. נשים לב כי $f(0)=f'(0)=0$ לכן לכל $0\le x\le 1$ יש $0\le\alpha\le x$ כך ש

$$e^{-x}-(1-x) = f(x)=\frac{f''(\alpha)x^2}{2}=\frac{e^{-\alpha}x^2}{2}\in\left[0,\frac{x^2}{2}\right]$$

נציב $x=\frac{t}{n}\in[0,1]$ ונקבל

$$0 \le e^{-\frac{t}{n}}-\left(1-\frac{t}{n}\right)\le\frac{t^2}{2n^2}$$

כעת נשתמש באי־שוויון

$$0\le a^n-b^n \le (a-b)\cdot n\cdot a^{n-1}$$

כאשר $a\geq b\geq 0$. נציב באי־שוויון זה $b=1-\frac{t}{n}$ ו $a=e^{-\frac{t}{n}}$ ונקבל

$$\begin{aligned}
0 & \leq \underbrace{e^{-t}}_{a^{n}}-\underbrace{\left(1-\frac{t}{n}\right)^{n}}_{b^{n}}\\
 & \leq n\left(e^{-\frac{t}{n}}-\left(1-\frac{t}{n}\right)\right)e^{-\frac{t}{n}(n-1)}\\
 & \leq n\left(\frac{t^{2}}{2n^{2}}\right)e^{-\frac{t}{n}(n-1)}\\
 & = \frac{t^{2}}{2n}e^{-t}e^{\frac{t}{n}}\\
\underbrace{}_{\substack{t\leq n\\ e^{\frac{t}{n}}\leq e^{1}}} & \leq \frac{e}{2}\cdot\frac{t^{2}e^{-t}}{n}
\end{aligned}$$

$\blacksquare$

נעבור להוכחת נוסחת המכפלה של אוילר: **הוכחה:** אנו רוצים להוכיח כי ל $z\in\mathbb{C}\setminus\{0,-1,-2,\dots\}$ מתקיים

$$\lim_{n\to\infty}\frac{(n-1)!\cdot n^{z}}{z(z+1)\dots(z+n-1)} = \Gamma(z)$$

אם נחליף את z ב $z+1$ אז צד ימין מוכפל ב z וצד שמאל מוכפל פי $\frac{z\cdot n}{z+n}\underset{n\to\infty}{\longrightarrow}z$. לכן אפשר להניח כי $\mathrm{Re}(z)\geq 1$. נסיק מטענת העזר כי

$$\begin{aligned}
\left|\int_{0}^{n}t^{z-1}e^{-t}dt-\int_{0}^{n}t^{z-1}\left(1-\frac{t}{n}\right)^{n}dt\right| & \leq \int_{0}^{n}\left|t^{z-1}\right|\left|e^{-t}-\left(1-\frac{t}{n}\right)^{n}\right|dt\\
 & \leq \int_{0}^{n}t^{\mathrm{Re}(z)-1}\cdot\frac{e}{2}\cdot\frac{t^{2}\cdot e^{-t}}{n}dt\\
 & \leq \frac{1}{n}\cdot\frac{e}{2}\cdot\int_{0}^{n}t^{\mathrm{Re}(z)+1}e^{-t}dt\underset{n\to\infty}{\longrightarrow}0
\end{aligned}$$

כי $\int_{0}^{n}t^{\mathrm{Re}(z)+1}e^{-t}dt\underset{n\to\infty}{\longrightarrow}\Gamma(\mathrm{Re}(z)+2)$. לכן

$$\lim_{n\to\infty}\int_{0}^{n}t^{z-1}\left(1-\frac{t}{n}\right)^{n}dt = \Gamma(z)$$

נציב $t=ns$ ונקבל

$$\begin{aligned}
\int_{0}^{n}t^{z-1}\left(1-\frac{t}{n}\right)^{n}dt & = \int_{0}^{1}n^{z-1}s^{z-1}(1-s)^{n}\cdot nds\\
 & = n^{z}\int_{0}^{1}s^{z-1}(1-s)^{n}ds
\end{aligned}$$

אם $n>0$ אז מתקיים

$$\begin{aligned}
\int_0^1 s^{z-1}(1-s)^n\,ds &= \int_0^1\left(\frac{s^z}{z}\right)'(1-s)^n\,ds\\
&= \frac{s^z}{z}(1-s)^n\,|_0^1-\int_0^1\left(\frac{s^z}{z}\right)\left((1-s)^n\right)'ds\\
&= 0+\frac{n}{z}\int_0^1 s^z(1-s)^{n-1}\,ds\\
&= \frac{n}{z}\int_0^1 s^z(1-s)^{n-1}\,ds\\
&= \frac{n(n-1)}{z(z+1)}\int_0^1 s^{z+1}(1-s)^{n-2}\,ds\\
&= \dots\\
&= \frac{n(n-1)\cdot\ldots\cdot 1}{z(z+1)\cdot\ldots\cdot(z+(n-1))}\int_0^1 s^{z+n-1}ds\\
&= \frac{n(n-1)\cdot\ldots\cdot 1}{z(z+1)\cdot\ldots\cdot(z+(n-1))}\left[\frac{s^{z+n}}{z+n}\right]|_0^1\\
&= \frac{n!}{z(z+1)\cdot\ldots\cdot(z+(n-1))(z+n)}
\end{aligned}$$

קיבלנו

$$\begin{aligned}
\Gamma(z) &= \lim_{n\to\infty}\int_0^n t^{z-1}\left(1-\frac{t}{n}\right)^n dt\\
&= \lim_{n\to\infty} n^z\int_0^1 s^{z-1}(1-s)^n\,ds\\
&= \lim_{n\to\infty}\frac{n^z\cdot n!}{z(z+1)\cdot\ldots\cdot(z+n)}
\end{aligned}$$

ע"י הכפלת שני האגפים ב$\lim_{n\to\infty}\frac{z+n}{n}=1$ נקבל את הנוסחה. ■

6. צורת ויירשטראס להופכי של Γ: Γ לא מתאפסת ולכן $\Gamma^{-1}=\frac{1}{\Gamma}$ פונקציה שלמה (הנקודות $0,-1,-2,\dots$ הם האפסים של Γ^{-1} והם פשוטים) ומתקיים

$$\Gamma^{-1}(z) = ze^{\gamma z}\prod_{n=1}^{\infty}\left(\left(1+\frac{z}{n}\right)e^{-\frac{z}{n}}\right)$$

כאשר

$$\begin{aligned}
\gamma &= \lim_{n\to\infty}\left(\sum_{k=1}^{n-1}\frac{1}{k}-\log n\right)\\
&= \lim_{n\to\infty}\sum_{k=1}^{n-1}\int_k^{k+1}\left(\frac{1}{k}-\frac{1}{t}\right)dt
\end{aligned}$$

הוא קבוע אוילר מסקרוני.

הוכחה:

$$\frac{z(z+1)\cdot\ldots\cdot(z+(n-1))}{(n-1)!\cdot n^z} = z\exp\left(z\left(\sum_{k=1}^{n-1}\frac{1}{k}-\log n\right)\right)\prod_{k=1}^{n-1}\left(\left(1+\frac{z}{k}\right)e^{-\frac{z}{k}}\right)$$

לכן נקבל מנוסחת המכפלה של אוילר

$$\frac{1}{\Gamma(z)} = \lim_{n\to\infty}\frac{z(z+1)\cdot\ldots\cdot(z+(n-1))}{(n-1)!\cdot n^z} =$$

$$\lim_{n\to\infty} z\exp\left(z\left(\sum_{k=1}^{n-1}\frac{1}{k}-\log n\right)\right)\prod_{k=1}^{n-1}\left(\left(1+\frac{z}{k}\right)e^{-\frac{z}{k}}\right) = ze^{\gamma z}\prod_{k=1}^{\infty}\left(1+\frac{z}{k}\right)e^{-\frac{z}{k}}$$

■

7. נוסחה נוספת:

$$\Gamma(z) = \frac{1}{z}\prod_{n=1}^{\infty}\left(\left(1+\frac{1}{n}\right)^z\left(1+\frac{z}{n}\right)^{-1}\right)$$

הוכחה: נשתמש בנוסחת המכפלה של אוילר

$$\frac{(n-1)!\cdot n^z}{z(z+1)\ldots(z+n-1)} = \frac{n^z}{z}\prod_{j=1}^{n-1}\left(1+\frac{z}{j}\right)^{-1}$$

נכתוב

$$\begin{aligned} n &= \frac{n}{n-1}\cdot\frac{n-1}{n-2}\cdot\ldots\cdot\frac{2}{1} = \left(1+\frac{1}{n-1}\right)\left(1+\frac{1}{n-2}\right)\cdot\ldots\cdot\left(1+\frac{1}{1}\right) \\ &= \prod_{j=1}^{n-1}\left(1+\frac{1}{j}\right) \end{aligned}$$

ולכן

$$\begin{aligned} \frac{(n-1)!\cdot n^z}{z(z+1)\ldots(z+n-1)} &= \frac{1}{z}\left(\prod_{j=1}^{n-1}\left(1+\frac{1}{j}\right)\right)^z\prod_{j=1}^{n-1}\left(1+\frac{z}{j}\right)^{-1} \\ &= \frac{1}{z}\prod_{j=1}^{n-1}\left(1+\frac{1}{j}\right)^z\left(1+\frac{z}{j}\right)^{-1} \end{aligned}$$

מכאן קיבלנו

$$\begin{aligned} \Gamma(z) &= \lim_{n\to\infty}\frac{(n-1)!\cdot n^z}{z(z+1)\ldots(z+n-1)} \\ &= \frac{1}{z}\prod_{j=1}^{\infty}\left(1+\frac{1}{j}\right)^z\left(1+\frac{z}{j}\right)^{-1} \end{aligned}$$

■

2 פונקציית בטא ושימושים לΓ

הגדרה 2.1 ל$a,b\in\mathbb{C}$ עם $\mathrm{Re}a>0$ ו$\mathrm{Re}b>0$ נגדיר

$$\mathrm{B}\left(a,b\right) = \int_{0}^{1}s^{a-1}\left(1-s\right)^{b-1}ds$$

2.1 תכונות

מבוסס על Notes on Riemann's zeta function של Dragan Milicic

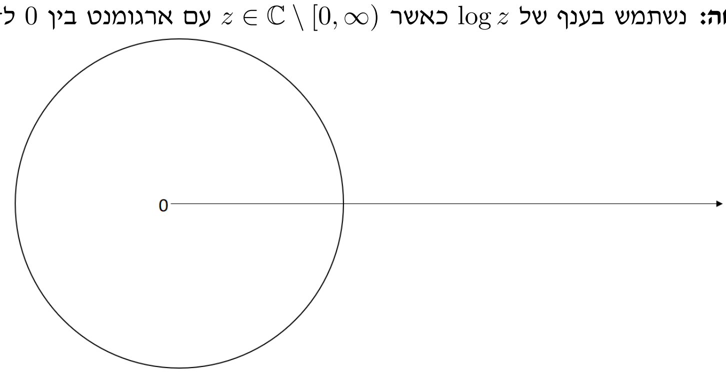
1. $\mathrm{B}\left(a,b\right)=\mathrm{B}\left(b,a\right)$
2. נציב $u=\frac{s}{1-s}=\frac{1}{1-s}-1$ ואז $u-us=s$ ולכן $s=\frac{u}{u+1}$ ולכן $s=1-\frac{1}{u+1}$, $\frac{ds}{du}=\frac{1}{(u+1)^{2}}$

$$\begin{aligned}\mathrm{B}\left(a,b\right) &= \int_{0}^{1}\left(\frac{1}{u+1}\right)^{b-1}\left(\frac{u}{u+1}\right)^{a-1}\frac{du}{\left(u+1\right)^{2}}\\ &= \int_{0}^{1}u^{a}\left(\frac{1}{u+1}\right)^{a+b}\cdot\frac{1}{u}du\end{aligned}$$

למה 2.2 נניח $0<\alpha<1$ אז

$$\int_{0}^{\infty}\frac{t^{-\alpha}}{1+t}dt = \frac{\pi}{\sin\left(\pi\alpha\right)}$$

הוכחה: נשתמש בענף של $\log z$ כאשר $z\in\mathbb{C}\setminus[0,\infty)$ עם ארגומנט בין 0 ל2π.



נסמן

$$f\left(z\right) = \frac{z^{-\alpha}}{1+z}=\frac{e^{-\alpha\log z}}{1+z}$$

בתחום $\mathbb{C}\setminus[0,\infty)$. נשים לב כי

$$\left|z^{-\alpha}\right| = \left|e^{-\alpha\log z}\right| = e^{-\alpha\mathrm{Re}(\log z)} = e^{-\alpha\log|z|} = |z|^{-\alpha}$$

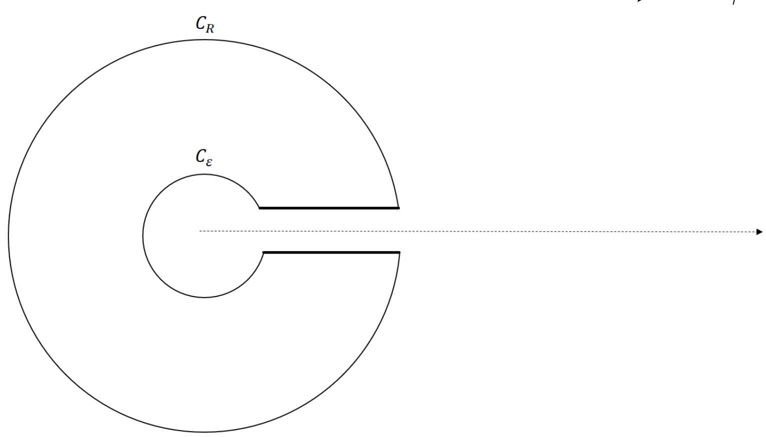
ל-f יש קוטב פשוט ב-$z=-1$ עם שארית

$$\mathrm{Res}_{z=-1}f(z) = e^{-\alpha\log(-1)} = e^{-\alpha\pi i}$$

לכן

$$\int_{\gamma}\frac{z^{-\alpha}}{1+z}dz = e^{-\alpha\pi i}$$

כאשר γ נתונה על ידי



ו-$R\nearrow\infty$ ו-$\varepsilon\searrow0$. מאחר ו-$0<\alpha<1$ מתקיים

$$\left|\int_{C_\varepsilon}\frac{z^{-\alpha}}{1+z}dz\right| \leq 2\pi\varepsilon\cdot\frac{\varepsilon^{-\alpha}}{1-\varepsilon}\xrightarrow[\varepsilon\to0]{}0$$
$$\left|\int_{C_R}\frac{z^{-\alpha}}{1+z}dz\right| \leq 2\pi R\cdot\frac{R^{-\alpha}}{R-1}\xrightarrow[R\to\infty]{}0$$

לכן

$$\frac{1}{2\pi i}\left(\int_0^\infty\frac{t^{-\alpha}}{1+t}dt-\int_0^\infty\frac{t^{-\alpha}}{1+t}e^{-\alpha(2\pi i)}dt\right) = e^{-\alpha\pi i}$$

כלומר

$$\int_0^\infty\frac{t^{-\alpha}}{1+t}dt = 2\pi i\cdot\frac{e^{-\alpha\pi i}}{1-e^{-2\alpha\pi i}} = \frac{2\pi i}{e^{\alpha\pi i}-e^{-\alpha\pi i}} = \frac{\pi}{\sin(\pi\alpha)}$$

■

מסקנה 2.3 אם $0<\alpha<1$ אז נקבל (אם נציב $\alpha=1-a$)

$$\begin{aligned}\mathrm{B}(a,1-a) &= \int_0^1 u^a\left(\frac{1}{u+1}\right)^{a+(1-a)}\cdot\frac{1}{u}du\\ &= \int_0^1 \frac{u^{a-1}}{u+1}du\\ &= \frac{\pi}{\sin(\pi(1-a))}=\frac{\pi}{\sin(\pi a)}\end{aligned}$$

טענה 2.4 (חישוב מיוחד נוסף)

$$\mathrm{B}(z,z) = 2^{1-2z}\mathrm{B}\left(z,\frac{1}{2}\right)$$

ל-$\mathrm{Re}z>0$.

הוכחה:

$$\begin{aligned}\mathrm{B}(z,z) &= \int_0^1 s^{z-1}(1-s)^{z-1}ds\\ &= 2\int_0^{\frac{1}{2}}[s(1-s)]^z\frac{1}{s(s-1)}ds\end{aligned}$$

כאשר השוויון האחרון נכון כי האינטגרל סימטרי. נציב $t=4s(1-s)$ כלומר $t:\left[0,\frac{1}{2}\right]\to[0,1]$ ומתקיים $\frac{dt}{ds}=4-8s=4(1-2s)=4\sqrt{1-t}$ (כי $1-t=1-4s+4s^2=(1-2s)^2$).
לכן

$$\frac{ds}{s(1-s)} = \frac{4ds}{t}=\frac{4}{t\cdot4\sqrt{1-t}}dt=\frac{1}{t\sqrt{1-t}}dt$$

ואז

$$\begin{aligned}\mathrm{B}(z,z) &= 2\int_0^{\frac{1}{2}}[s(1-s)]^z\frac{1}{s(s-1)}ds\\ &= 2\int_0^1\left(\frac{t}{4}\right)^z\frac{1}{t\sqrt{t-1}}dt\\ &= 2^{1-2z}\int_0^1 t^z(1-t)^{-\frac{1}{2}}dt\\ &= 2^{1-2z}\mathrm{B}\left(z,\frac{1}{2}\right)\end{aligned}$$

■

2.2 קשר בין Γ לבין B

נניח כי $0<\mathrm{Re}\left(a\right),\mathrm{Re}\left(b\right)$ אז

$$\Gamma\left(a\right)\Gamma\left(b\right) = \int_{0}^{\infty}\left(\int_{0}^{\infty}e^{-(t+s)}s^{a}t^{b}\frac{ds}{s}\right)\frac{dt}{t}$$

לכל $t>0$ נציב $s=tu$ (ואז $\frac{ds}{du}=t$) באינטגרל הפנימי ונקבל

$$\int_{0}^{\infty}\left(\int_{0}^{\infty}e^{-(t+tu)}\left(tu\right)^{a}t^{b}\frac{tdu}{tu}\right)\frac{dt}{t} = \int_{0}^{\infty}\left(\int_{0}^{\infty}e^{-(1+u)t}t^{a+b}u^{a}\right)\frac{dt}{t}\frac{du}{u}$$

לכל $u>0$ נציב $t=\frac{x}{1+u}$ ($\frac{dt}{dx}=\frac{1}{1+u}$) באינטגרל הפנימי ונקבל

$$\begin{aligned} &= \int_{0}^{\infty}\left(\int_{0}^{\infty}e^{-x}\left(\frac{x}{1+u}\right)^{a+b}u^{a}\right)\left(1+u\right)\frac{dx}{x\left(1+u\right)}\frac{du}{u}\\ &= \int_{0}^{\infty}\left(\int_{0}^{\infty}e^{-x}\left(\frac{x}{1+u}\right)^{a+b}u^{a}\right)\frac{dx}{x}\frac{du}{u}\\ &= \underbrace{\int_{0}^{\infty}e^{-x}x^{a+b}\frac{1}{x}dx}_{\Gamma(a+b)}\cdot\underbrace{\int_{0}^{\infty}u^{a}\left(\frac{1}{1+u}\right)^{a+b}\frac{du}{u}}_{\mathrm{B}(a,b)}\end{aligned}$$

לכן קיבלנו $\Gamma\left(a\right)\Gamma\left(b\right)=\Gamma\left(a+b\right)\mathrm{B}\left(a,b\right)$ כלומר

$$\mathrm{B}\left(a,b\right) = \frac{\Gamma\left(a\right)\Gamma\left(b\right)}{\Gamma\left(a+b\right)}$$

טענה 2.5 (נוסחת השיקוף של אוילר):

$$\Gamma\left(z\right)\Gamma\left(1-z\right) = \frac{\pi}{\sin\left(\pi z\right)}$$

הוכחה: ממשפט היחידות בפונקציות מרוכבות, די להוכיח זאת עבור $0<z<1$. מתקיים

$$\mathrm{B}\left(z,1-z\right) = \frac{\Gamma\left(z\right)\Gamma\left(1-z\right)}{\Gamma\left(1-z+z\right)}=\Gamma\left(z\right)\Gamma\left(1-z\right)$$

והוכחנו כי ל$0<z<1$ מתקיים

$$\mathrm{B}\left(z,1-z\right) = \frac{\pi}{\sin\left(\pi z\right)}$$

כנדרש. ■

מסקנה 2.6 (מקרה פרטי): $\sqrt{\pi}=\Gamma\left(\frac{1}{2}\right)$ כי $\pi=\Gamma\left(\frac{1}{2}\right)^{2}$ ומתקיים כי $\Gamma\left(\frac{1}{2}\right)=\int_{0}^{\infty}t^{\frac{1}{2}-1}e^{-t}dt\geq0$.

טענה 2.7 (נוסחת הדופליקציה של לז'נדר):

$$\Gamma\left(2z\right)=\frac{2^{2z-1}}{\sqrt{\pi}}\Gamma\left(z\right)\Gamma\left(z+\frac{1}{2}\right)$$

הוכחה: נניח כי $\mathrm{Re}\left(z\right)>0$. אז

$$\frac{\Gamma\left(z\right)\Gamma\left(z\right)}{\Gamma\left(2z\right)}=\mathrm{B}\left(z,z\right)=2^{1-2z}\mathrm{B}\left(z,\frac{1}{2}\right)$$

מצד שני

$$\mathrm{B}\left(z,\frac{1}{2}\right)=\frac{\Gamma\left(z\right)\Gamma\left(\frac{1}{2}\right)}{\Gamma\left(z+\frac{1}{2}\right)}$$

לכן

$$\frac{\Gamma\left(z\right)\Gamma\left(z\right)}{\Gamma\left(2z\right)}=2^{1-2z}\frac{\Gamma\left(z\right)\Gamma\left(\frac{1}{2}\right)}{\Gamma\left(z+\frac{1}{2}\right)}=2^{1-2z}\frac{\Gamma\left(z\right)\sqrt{\pi}}{\Gamma\left(z+\frac{1}{2}\right)}$$

ולכן

$$\Gamma\left(2z\right)=\frac{2^{2z-1}\Gamma\left(z\right)\Gamma\left(z+\frac{1}{2}\right)}{\sqrt{\pi}}$$

■

הערה 2.8 בהמשך נשתמש בעיקר בשתי הזהויות

$$\Gamma\left(z\right)\Gamma\left(1-z\right)=\frac{\pi}{\sin\left(\pi z\right)}$$

$$\Gamma\left(2z\right)=\frac{2^{2z-1}}{\sqrt{\pi}}\Gamma\left(z\right)\Gamma\left(z+\frac{1}{2}\right)$$

3 פונקציית ζ

הגדרה 3.1 יהי $z\in\mathbb{C}$ עם $\mathrm{Re}z>1$. נגדיר

$$\zeta\left(z\right)=\sum_{n=1}^{\infty}\frac{1}{n^{z}}$$

הערה 3.2 (תזכורת): אם $t>0$ אז $|t^z|=t^{\mathrm{Re}z}$

טענה 3.3 לכל $\varepsilon>0$ הטור מתכנס בהחלט במידה שווה על $\mathrm{Re}z>1+\varepsilon$ ולכן מתאר פונקציה הולומורפית ב$\mathrm{Re}z>1$.

הוכחה: מהשוואה לטור $\sum_{n=1}^{\infty}\frac{1}{n^{1+\varepsilon}}$ ושימוש במשפט ויירשטראס. ■

3.1 פירוק אוילר

טענה 3.4

$$\zeta(z) = \prod_{p\text{ is prime}}\frac{1}{1-\frac{1}{p^z}}$$

הוכחה: מתקיים

$$\begin{aligned}\zeta(z) &= \lim_{k\to\infty}\sum_{\substack{n\\ n\text{ divides only}\\ p_1,\dots,p_k}}\frac{1}{n^z}\\ &= \lim_{k\to\infty}\left(1+\frac{1}{p_1^z}+\frac{1}{p_1^{2z}}+\dots\right)\dots\left(1+\frac{1}{p_k^z}+\frac{1}{p_k^{2z}}+\dots\right)\\ &= \lim_{k\to\infty}\prod_{j=1}^{k}\frac{1}{1-\frac{1}{p_j^z}}\\ &= \prod_{j=1}^{\infty}\frac{1}{1-\frac{1}{p_j^z}}\end{aligned}$$

■

הערה 3.5 המכפלה מתכנסת בהחלט: נסמן

$$\frac{1}{1-\frac{1}{p^z}}=1+f_p(z)\qquad(\mathrm{Re}(z)>1)$$

נקח $\delta>0$. עבור $\mathrm{Re}z>1+\delta$ נקבל

$$|f_p(z)| = \left|\frac{\frac{1}{p^z}}{1-\frac{1}{p^z}}\right|\le\frac{1}{p^{1+\delta}}\frac{1}{1-\frac{1}{2^{1+\delta}}}\le\frac{2}{p^{1+\delta}}$$

מאחר ו

$$\sum_{p\text{ is prime}}\frac{2}{p^{1+\delta}} < \sum_{n=1}^{\infty}\frac{2}{n^{1+\delta}}<\infty$$

נקבל שהמכפלה מתכנסת בהחלט, ומכאן נובע שלζ אין אפסים ב$\mathrm{Re}z>1$.

3.2 כפל עם Γ

בעזרת ההצבה $t=ns$ נקבל (ל $\mathrm{Re}z>1$, $n=1,2,\ldots$)

$$\begin{aligned}\Gamma(z) &= \int_0^\infty t^{z-1}e^{-t}dt\\ &= \int_0^\infty (ns)^{z-1}e^{-ns}nds\\ &= n^z\int_0^\infty s^{z-1}e^{-ns}ds\end{aligned}$$

לכן

$$\frac{\Gamma(z)}{n^z} = \int_0^\infty t^{z-1}e^{-nt}dt$$

לכן (קודם פורמלית):

$$\begin{aligned}\Gamma(z)\zeta(z) &= \sum_{n=1}^\infty \frac{\Gamma(z)}{n^z}\\ &= \sum_{n=1}^\infty\int_0^\infty t^{z-1}e^{-nt}dt\\ &= \int_0^\infty\sum_{n=1}^\infty t^{z-1}e^{-nt}dt\\ &= \int_0^\infty t^{z-1}\frac{e^{-t}}{1-e^{-t}}dt\\ &= \int_0^\infty t^{z-1}\frac{1}{e^t-1}dt\end{aligned}$$

והאינטגרל האחרון מתכנס בהחלט עבור $\mathrm{Re}z>1$.

הערה 3.6 מותר להחליף את האינטגרל ואת הסכום כי

$$\sum_{n=1}^\infty\int_0^\infty\left|t^{z-1}e^{-nt}\right|dt = \int_0^\infty |t|^{\mathrm{Re}(z)-1}\frac{1}{e^t-1}dt<\infty$$

(וזה נכון כי כאן מותר להחליף אינטגרל וסכום כי כל הביטויים חיוביים)

3.3 ההרחבה המרומורפית לפי רימן

(מבוסס על Riemann's Zeta Function: Harold M. Edwards.)

עבור $u\in\mathbb{C}\setminus(-\infty,0]$ נגדיר ענף $\log u=\log|u|+i\arg u$ עם $\arg u\in(-\pi,\pi]$.
נתייחס ל

$$I(z) = \int_{\gamma_{\varepsilon,\delta}}\frac{(-u)^z}{e^u-1}\frac{du}{u}$$

כאשר $\mathrm{Re} z > 1$. (להוסיף ציור של $\gamma_{\varepsilon,\delta}$)
כאשר $\varepsilon \to 0^+$ מתקיים

$$\begin{aligned} I_1 \quad & \underset{\varepsilon\to 0^+}{\longrightarrow} \quad -\int_\delta^\infty \frac{e^{z(\log t - i\pi)}}{e^t-1}\frac{dt}{t} \\ & = \quad -e^{-i\pi z}\int_\delta^\infty \frac{t^{z-1}}{e^t-1}dt \end{aligned}$$

באופן דומה

$$\begin{aligned} I_3 \quad & \underset{\varepsilon\to 0^+}{\longrightarrow} \quad \int_\delta^\infty \frac{e^{z(\log t + i\pi)}}{e^t-1}\frac{dt}{t} \\ & = \quad e^{i\pi z}\int_\delta^\infty \frac{t^{z-1}}{e^t-1}dt \end{aligned}$$

לבסוף

$$\begin{aligned} I_2 \quad & \underset{\varepsilon\to 0^+}{\longrightarrow} \quad \int_{C_\delta} \frac{(-u)^z}{e^u-1}\frac{du}{u} \\ \left|\int_{C_\delta} \frac{(-u)^z}{e^u-1}\frac{du}{u}\right| \quad & = \quad \left|\int_{C_\delta} \frac{u}{e^u-1}\frac{(-u)^z}{u}\frac{du}{u}\right| \end{aligned}$$

מתקיים כי הפונקציה $\frac{z}{e^z-1}$ רציפה בסביבה מספיק קטנה של הראשית ובפרט חסומה.
מתקיים $\left|\frac{(-u)^z}{u}\right| = \delta^{\mathrm{Re}z-1}$ לכל $z \in C_\delta$. לכן

$$\begin{aligned} |I_2| \quad & = \quad \left|\int_{C_\delta} \frac{(-u)^z}{e^u-1}\frac{du}{u}\right| \\ & \leq \quad \mathrm{const}\cdot \delta^{\mathrm{Re}z-1}\cdot \int_{C_\delta}\frac{du}{u} \\ & = \quad \mathrm{const}\cdot \delta^{\mathrm{Re}z-1}\cdot 2\pi \underset{\delta\to 0}{\longrightarrow} 0 \end{aligned}$$

בסה"כ קיבלנו

$$\begin{aligned} I(z) = \int_{\gamma_{\varepsilon,\delta}} \frac{(-u)^z}{e^u-1}\frac{du}{u} \quad & \underset{\varepsilon,\delta\to 0}{\longrightarrow} \quad \left(e^{i\pi z} - e^{-i\pi z}\right)\int_0^\infty \frac{t^{z-1}}{e^t-1}dt \\ & = \quad 2i\sin(\pi z)\cdot\Gamma(z)\zeta(z) \\ \underbrace{\qquad}_{\Gamma(z)\Gamma(1-z)=\frac{\pi}{\sin(\pi z)}} \quad & = \quad \frac{2\pi i}{\Gamma(1-z)}\zeta(z) \end{aligned}$$

פונקציה זו אינה תלויה ε,δ כאשר ε,δ קטנים מספיק, מאחר ו$\frac{(-u)^z}{e^u-1}$ הולומורפית ולכן מתאפסת על מסילות סגורות, ובנוסף על קווים אנכיים רחוקים מספיק מתקיים כי האינטגרל שואף ל0.
ראינו כי

$$\Gamma(z)\zeta(z) \quad = \quad \int_0^\infty \frac{t^{z-1}}{e^t-1}dt$$

מתקיים כי ל$\text{Re}z>1$

$$\zeta\left(z\right)=\frac{1}{2\pi i}\Gamma\left(1-z\right)\int_{\gamma_{\varepsilon,\delta}}\frac{\left(-u\right)^{z}}{e^{u}-1}\frac{du}{u}$$

ובנוסף $I\left(z\right)=\int_{\gamma_{\varepsilon,\delta}}\frac{\left(-u\right)^{z}}{e^{u}-1}\frac{du}{u}$ היא פונקציה שלמה - ניתן להסביר זאת ע"י שימוש במשפט מוררה.

מאחר ו$\Gamma\left(1-z\right)$ מרומורפית על $\mathbb{C}$ עם קטבים כאשר $1-z=0,-1,-2,\ldots$ כלומר כאשר $z=1,2,3,\ldots$ ומאחר ו$z\mapsto\int_{\gamma_{\varepsilon,\delta}}\frac{\left(-u\right)^{z}}{e^{u}-1}\frac{du}{u}$ היא פונקציה שלמה, נקבל כי לζ יש המשכה מרומורפית ל$\mathbb{C}$ לכל היותר קטבים פשוטים בנקודות $z=1,2,3,\ldots$. אבל לפי ההגדרה ζ הולומורפית ב$\text{Re}z>1$. לכן ζ מרומורפית על $\mathbb{C}$ עם לכל היותר קוטב פשוט $z=1$. אכן זה קוטב כי:

$$\zeta\left(1\right)=\lim_{s\to1^{+}}\zeta\left(s\right)=\lim_{s\to1^{+}}\sum_{n=1}^{\infty}\frac{1}{n^{s}}=\sum_{n=1}^{\infty}\frac{1}{n}=\infty$$

הערה 3.7 מתקיים למעשה $\text{Res}_{z=1}\zeta\left(z\right)=1$

הוכחה: די לבדוק כי $\zeta\left(t\right)-\frac{1}{t-1}$ חסומה ב$(1,2)$. אבל ל$t>1$ מתקיים

$$\int_{1}^{\infty}\frac{ds}{s^{t}}=\frac{s^{1-t}}{1-t}\Big|_{s=1}^{\infty}=-\frac{1}{1-t}=\frac{1}{t-1}$$

לכן צריך לבדוק כי $t\mapsto\left(\sum_{n=1}^{\infty}\frac{1}{n^{t}}-\int_{1}^{\infty}\frac{ds}{s^{t}}\right)$ חסומה ב$(1,2)$. וזה נכון לפי ציור. ■

3.4 אי־התאפסות ζ עבור $\text{Re}z=1$

3.4.1 הכנות

1. נגזרת לוגריתמית:

הגדרה 3.8 הנגזרת הלוגריתמית של פונקציה הולומורפית f היא הפונקציה $\frac{f'}{f}$.

מתקיימות התכונות הבאות:

- $\frac{(fg)'}{fg}=\frac{f'}{f}+\frac{g'}{g}$
- $\frac{\left(f^{k}\right)'}{f^{k}}=k\frac{f'}{f}$
- $\frac{\left(\frac{1}{f}\right)'}{\frac{1}{f}}=-\frac{f'}{f}$

2. אם f הולומורפית סביב $z_{0}=x_{0}+iy_{0}$ (ולא זהותית 0), ואם $f\left(z_{0}\right)=0$ אז קיים $\varepsilon>0$ כך שעבור $z=x+iy_{0}$ עם $x_{0}<x<x_{0}+\varepsilon$ מתקיים $\text{Re}\left(\left(\frac{f'}{f}\right)\left(z\right)\right)>0$.

הוכחה: אכן, יש פירוק $f(z)=c(z-z_0)^k(1+a_1z+\dots)$ עם $c\neq 0$ ו$k>0$ ואז

$$\left(\frac{f'}{f}\right)(z_0) = \frac{k}{z-z_0}+\frac{a_1+\dots}{1+a_1z+\dots}$$

ומכאן נובעת הטענה (כי $\lim_{x\to x_0^+}\mathrm{Re}\left(\frac{f'}{f}\right)(x+iy_0)=+\infty$) ■

3. אם p ראשוני ו$f(z)=\frac{1}{1-p^{-z}}$, נסמן $g(z)=1-p^{-z}$ ואז

$$\begin{aligned}\left(\frac{f'}{f}\right)(z_0) &= -\left(\frac{g'}{g}\right)(z)=-\frac{\left(1-e^{-z\log p}\right)'}{1-e^{-z\log p}}=-\frac{\log p\cdot e^{-z\log p}}{1-e^{-z\log p}}\\ &= -\frac{\log p\cdot p^{-z}}{1-p^{-z}}=-\log p\sum_{j=1}^{\infty}p^{-jz}\end{aligned}$$

3.4.2 פונקציית Λ

הגדרה 3.9 נגדיר פונקציה $\Lambda:\{1,2,3,\dots\}\to\mathbb{R}$ ע"י

$$\Lambda(n) = \begin{cases}\log p & n=p^k,k\geq 1,p\text{ is prime}\\ 0 & \text{otherwise}\end{cases}$$

בפרט $\Lambda(1)=0$

טענה 3.10 ל$\mathrm{Re}z>1$ מתקיים

$$\left(\frac{\zeta'}{\zeta}\right)(z) = -\sum_{n=1}^{\infty}\Lambda(n)\cdot n^{-z}$$

הערה 3.11 הטור הנ"ל מתכנס בהחלט ובמידה שווה על כל $\mathrm{Re}z>1+\delta$ לכל $\delta>0$ כי הוא חסום ע"י $\left|\log n\cdot\frac{1}{n^z}\right|=\log n\cdot\frac{1}{n^{\mathrm{Re}z}}<\log n\cdot\frac{1}{n^{1+\delta}}$.

הוכחה: (של הטענה): נסדר את המספרים הראשוניים בסדרה $\{p_n\}_{n=1}^{\infty}$. אז

$$\prod_{n=1}^{N}\frac{1}{1-p_n^{-z}} \longrightarrow \zeta(z)$$

במידה שווה על קבוצות קומפקטיות ב$\mathrm{Re}z>1$. לכן גם

$$\prod_{n=1}^{N}\frac{1}{1-p_n^{-z}} \longrightarrow \zeta'(z)$$

במידה שווה על קבוצות קומפקטיות ב$\mathrm{Re}z>1$. מכיוון ש$\zeta\neq 0$ על $\mathrm{Re}z>1$ נובע ש

$$-\sum_{n=1}^{N}\log p_n\sum_{j=1}^{\infty}p_n^{-jz} = \frac{\left(\prod_{n=1}^{N}\frac{1}{1-p_n^{-z}}\right)'}{\left(\prod_{n=1}^{N}\frac{1}{1-p_n^{-z}}\right)}\longrightarrow\frac{\zeta'(z)}{\zeta(z)}$$

ולכן

$$\left(\frac{\zeta'}{\zeta}\right)(z) = -\sum_{p}\log p\sum_{j=1}^{\infty}p^{-jz}=-\sum_{n=1}^{\infty}\Lambda(n)\,n^{-z}$$

ל$\mathrm{Re}z>1$. ■

3.4.3 אי־שוויון של $\cos$

למה 3.12 לכל α ממשי מתקיים $3+4\cos\alpha+\cos(2\alpha)\geq 0$.

הוכחה: אכן

$$\begin{aligned}3+4\cos\alpha+\cos(2\alpha) &= 3+4\cos\alpha+2\cos^2\alpha-1\\ &= 2\left(1+2\cos\alpha+\cos^2\alpha\right)\\ &= 2\left(1+\cos\alpha\right)^2\geq 0\end{aligned}$$

■

3.4.4 לζ אין אפסים על $\mathrm{Re}z=1$

טענה 3.13 לζ אין אפסים על $\mathrm{Re}z=1$

הוכחה: נניח בשלילה כי $1+it$ הוא אפס של ζ (כאשר t ממשי). $t\neq 0$ כי לζ יש קוטב ב$z=1$. נגדיר פונקציה מרומורפית על $\mathbb{C}$ על ידי

$$g(z) = \zeta(z)^3\cdot\zeta(z+it)^4\cdot\zeta(z+2it)$$

מאחר ו$z=1$ הוא קוטב פשוט של $\zeta(z)$, ואפס של $\zeta(z+it)$ ונקודה רגולרית של $\zeta(z+2it)$, נובע ש$z=1$ אפס של g ולכן עבור $\varepsilon>0$ קטן דיו, $\mathrm{Re}\left(\frac{g'}{g}(1+\varepsilon)\right)>0$. אבל עבור $\mathrm{Re}z>0$ מתקיים

$$\begin{aligned}\left(\frac{g'}{g}\right)(z) &= -\sum_{n=1}^{\infty}\Lambda(n)\left(3n^{-z}+4n^{-(z+it)}+n^{-(z+2it)}\right)\\ &= -\sum_{n=1}^{\infty}\Lambda(n)\,n^{-z}\left(3+4e^{-it\cdot\log n}+n^{-2it\cdot\log n}\right)\end{aligned}$$

ולכן

$$\mathrm{Re}\left(\left(\frac{g'}{g}\right)(1+\varepsilon)\right) = -\sum_{n=1}^{\infty}\Lambda(n)\,n^{-(1+\varepsilon)}\left(3+4\cos(t\cdot\log n)+\cos(2t\cdot\log n)\right)\leq 0$$

סתירה. ■

3.5 המשוואה הפונקציונלית - ההוכחה הראשונה של רימן

(מבוסס על Eduards)

נחזור לנוסחה

$$\zeta(z) = \frac{\Gamma(1-z)}{2\pi i}\int_{\gamma}\frac{(-u)^{z}}{e^{u}-1}\frac{du}{u}$$

כאשר $(-u)^{z}=e^{z\log(-u)}$. נקח $0<\varepsilon$ "קטן" ($\varepsilon<2\pi$). הנוסחה הנ"ל נכונה לכל z - כך הרחבנו את ζ. נניח כי $z<0$ ממשי, אז

$$\left|(-u)^{z}\right| = e^{z\mathrm{Re}\log(-u)}=|u|^{z}$$

נסתכל על האינטגרל

$$I_{n} = \frac{1}{2\pi i}\int_{C_{n}}\frac{(-u)^{z}}{e^{u}-1}\frac{du}{u}$$

כאשר C_{n} נתון ע"י ציור.

על C_{n}' קיים קבוע שאינו תלוי בn כך ש$K\le|e^{u}-1|$ ולכן

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{C_{n}'}\frac{(-u)^{z}}{e^{u}-1}\frac{du}{u}\right| &\le \frac{1}{2\pi}\cdot\max_{u\in C_{n}'}\left|\frac{(-u)^{z}}{e^{u}-1}\right|\cdot\left|\int_{C_{n}'}\frac{du}{u}\right|\\ &\le \frac{1}{2\pi}\frac{(\pi(2n+1))^{z}}{K}\cdot2\pi\underset{n\to\infty}{\longrightarrow}0\end{aligned}$$

(כזכור, $z<0$)

מתקיים

$$I_{n} \underset{n\to\infty}{\longrightarrow} -\frac{1}{2\pi i}\int_{\gamma}\frac{(-u)^{z}}{e^{u}-1}\frac{du}{u}=-\frac{\zeta(z)}{\Gamma(1-z)}$$

כאשר המינוסים כאן הם בגלל הכיוון של המסילה.

הקטבים של ההעתקה $u\to\frac{(-u)^{z}}{(e^{u}-1)u}=-\frac{(-u)^{z-1}}{e^{u}-1}$ הם בנקודות $u=2\pi ik$ עם $k=\pm1,\pm2,\pm3,\ldots,\pm n$. נחשב את השארית בנקודות אלה:

$$\begin{aligned}\mathrm{Res}_{u=2\pi ik}-\frac{(-u)^{z-1}}{e^{u}-1} &= \frac{-(-u)^{z-1}}{(e^{u}-1)'}\,|_{u=2\pi ik}\\ &= \frac{-(-u)^{z-1}}{e^{u}}\,|_{u=2\pi ik}\\ &= -(-2\pi ik)^{z-1}\end{aligned}$$

ולכן

$$\begin{aligned} I_n &= \sum_{\substack{k=-n \\ k\neq 0}}^{n} -\left(-2\pi i k\right)^{z-1} \\ &= \sum_{\substack{k=-n \\ k\neq 0}}^{n} -\left(-2\pi i k\right)^{z-1} \\ &= -\left(2\pi\right)^{z-1}\left(\sum_{k=1}^{n} k^{z-1}\left(i^{z-1}+\left(-i\right)^{z-1}\right)\right) \end{aligned}$$

אבל

$$\begin{aligned} i^{z-1}+\left(-i\right)^{z-1} &= \frac{i^{z}-\left(-i\right)^{z}}{i} \\ &= \frac{e^{z\log i}-e^{-z\log i}}{i} \\ &= 2\cdot\frac{e^{z\cdot\frac{\pi i}{2}}-e^{-z\cdot\frac{\pi i}{2}}}{2i} \\ &= 2\sin\left(\frac{\pi z}{2}\right) \end{aligned}$$

בסה"כ קיבלנו

$$I_n = -\left(2\pi\right)^{z-1} 2\sin\left(\frac{\pi z}{2}\right)\sum_{k=1}^{n} k^{z-1} \underset{n\to\infty}{\longrightarrow} -\left(2\pi\right)^{z-1} 2\sin\left(\frac{\pi}{2}\right)\zeta\left(1-z\right)$$

כי $z<0$ ממשי ולכן $1-z>1$ ממשי. בסה"כ נובע כי

$$\zeta\left(z\right) = \Gamma\left(1-z\right)\left(2\pi\right)^{z-1} 2\sin\left(\frac{\pi z}{2}\right)\zeta\left(1-z\right)$$

שעבור $z<0$ ממשי. מצד שני, שני הצדדים הם פונקציות מרומורפיות ולכן עבור כל z מתקיים השוויון.

מסקנה 3.14 נקח $\mathrm{Re}z<0$, אז $1<\mathrm{Re}\left(1-z\right)$ ולכן ל$\Gamma\left(1-z\right)$ ול$\zeta\left(1-z\right)$ אין אפס או קוטב בz. לכן לζ אין קטבים ב$\mathrm{Re}z<0$, והאפסים הם כמו של $\sin\left(\frac{\pi z}{2}\right)$, כלומר $z=-2,-4,-6,\ldots$. אלה נקראים האפסים הטריוואליים. כל שאר האפסים הם ב $0\le\mathrm{Re}z<1$, והשערת רימן היא שהם ב$\mathrm{Re}z=\frac{1}{2}$.

מסקנה 3.15 נקח $z=0$: אז ל$\zeta\left(1-z\right)$ יש קוטב פשוט ול$\sin\left(\frac{\pi z}{2}\right)$ אפס פשוט בנקודה זו, ול$\Gamma\left(1-z\right)$ לא קוטב ולא אפס ב$z=0$. לכן $z=0$ אינו אפס של ζ. נניח כי $\mathrm{Re}z_0=0$ ו$z_0\neq0$. ראינו כי ל$\zeta\left(1-z\right)$ אין אפס או קוטב ב$z=z_0$, ואותה תכונה מתקיימת עבור $\sin\left(\frac{\pi z}{2}\right)$ ו$\Gamma\left(1-z\right)$. מכאן לζ אין אפסים ב$\mathrm{Re}z=0$.

מסקנה 3.16 נקח z_0 עם $0<\mathrm{Re}z_0<1$. ל$\sin\left(\frac{\pi z}{2}\right)$ ול$\Gamma\left(1-z\right)$ אין אפס או קוטב ב$z=z_0$ ולכן z_0 אפס של ζ אם ורק אם $1-z_0$ אפס של ζ.

3.6 צורה סימטרית למשוואה הפונקציונלית

לפי נוסחת השיקוף

$$\sin\left(\frac{\pi z}{2}\right) = \frac{\pi}{\Gamma\left(\frac{z}{2}\right)\Gamma\left(1-\frac{z}{2}\right)}$$

לכן

$$\zeta(z) = \Gamma(1-z)(2\pi)^z \cdot \frac{1}{\Gamma\left(\frac{z}{2}\right)\Gamma\left(1-\frac{z}{2}\right)} \cdot \zeta(1-z)$$

על פי נוסחת הדולפיקציה

$$\begin{aligned}\Gamma(1-z) &= \Gamma\left(2\left(\frac{1-z}{2}\right)\right)\\ &= \frac{2^{2\left(\frac{1-z}{2}\right)-1}}{\sqrt{\pi}}\Gamma\left(\frac{1-z}{2}\right)\Gamma\left(\frac{1-z}{2}+\frac{1}{2}\right)\\ &= \frac{2^{-z}}{\sqrt{\pi}}\Gamma\left(\frac{1-z}{2}\right)\Gamma\left(1-\frac{z}{2}\right)\end{aligned}$$

לכן

$$\begin{aligned}\zeta(z) &= \frac{2^{-z}}{\sqrt{\pi}}\Gamma\left(\frac{1-z}{2}\right)\Gamma\left(1-\frac{z}{2}\right)(2\pi)^z \cdot \frac{1}{\Gamma\left(\frac{z}{2}\right)\Gamma\left(1-\frac{z}{2}\right)} \cdot \zeta(1-z)\\ &= \pi^{z-\frac{1}{2}}\frac{\Gamma\left(\frac{1-z}{2}\right)}{\Gamma\left(\frac{z}{2}\right)}\zeta(1-z)\\ &= \frac{\pi^{-\left(\frac{1-z}{2}\right)}\Gamma\left(\frac{1-z}{2}\right)\zeta(1-z)}{\pi^{-\frac{z}{2}} \cdot \Gamma\left(\frac{z}{2}\right)}\end{aligned}$$

בסה"כ קיבלנו

$$\pi^{-\frac{z}{2}}\Gamma\left(\frac{z}{2}\right)\zeta(z) = \pi^{-\frac{1-z}{2}}\Gamma\left(\frac{1-z}{2}\right)\zeta(1-z)$$

כלומר הפונקציה $\pi^{-\frac{z}{2}}\Gamma\left(\frac{z}{2}\right)\zeta(z)$ אינווריאנטית לטרנספורמציה $z \mapsto 1-z$.

4 המשוואה הפונקציונלית θ

4.1 נוסחת פואסון

4.1.1 סימונים לטרנספורם פוריה

נסמן

$$\hat{f}(\omega) = \int_{-\infty}^{\infty} f(t)\, e^{-2\pi i\omega t} dt$$

4.1.2 נוסחת פואסון

(ראה גם Dym, McKean)

טענה 4.1 תהי $f:(-\infty,\infty)\to\mathbb{C}$ בעלת שתי נגזרות רציפות על $(-\infty,\infty)$ ומקיימת

$$|f(x)|,|f'(x)|,|f''(x)| \leq \frac{C}{1+x^2}$$

כאשר $x\in\mathbb{R}$ ו$C>0$ קבוע. אז

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty}\hat{f}(n)$$

אנו נוכיח את הגרסה היותר כללית

$$\sum_{n=-\infty}^{\infty} f(n+t) = \sum_{n=-\infty}^{\infty}\hat{f}(n)e^{2\pi int}$$

הוכחה: נסמן

$$\varphi(t) = \sum_{n=-\infty}^{\infty} f(t+n)$$

אז מהתנאים על f נובע כי φ מחזורית בעלת מחזור 1, ובעלת נגזרת רציפה. לכן ניתן לפתח את φ לטור פוריה (חדו"א 2) ו

$$\varphi(t) = \sum_{k=-\infty}^{\infty} c_k e^{2\pi ikt}$$

כאשר

$$\begin{aligned}
c_k &= \left\langle\varphi, e^{2\pi ik\cdot}\right\rangle\\
&= \int_0^1 \varphi(t)e^{-2\pi ikt}dt\\
&= \int_0^1\sum_{n=-\infty}^{\infty} f(t+n)e^{-2\pi ikt}dt\\
&= \sum_{n=-\infty}^{\infty}\int_0^1 f(t+n)e^{-2\pi ikt}dt\\
&= \sum_{n=-\infty}^{\infty}\int_0^1 f(t+n)e^{-2\pi ik(t+n)}dt\\
&= \sum_{n=-\infty}^{\infty}\int_n^{n+1} f(t)e^{-2\pi ikt}dt\\
&= \int_{-\infty}^{\infty} f(t)e^{-2\pi ikt}dt\\
&= \hat{f}(k)
\end{aligned}$$

ובסה"כ קיבלנו

$$\varphi(t) = \sum_{n=-\infty}^{\infty} f(t+n) = \sum_{k=-\infty}^{\infty} \hat{f}(k) e^{2\pi ikt}$$

■

4.2 חישוב טרנספורם פוריה של פונקציה גאוסית

נסמן

$$I = \int_{-\infty}^{\infty} e^{-\frac{x^2}{2}} dx$$

אז

$$\begin{aligned} I^2 &= \int_{-\infty}^{\infty} e^{-\frac{x^2}{2}} dx \cdot \int_{-\infty}^{\infty} e^{-\frac{y^2}{2}} dy \\ &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e^{-\frac{x^2+y^2}{2}} dxdy \\ &= \int_{0}^{2\pi} \int_{0}^{\infty} e^{-\frac{r^2}{2}} rdrd\theta \\ &= 2\pi \cdot \left(-e^{-\frac{r^2}{2}}\right) |_0^\infty \\ &= 2\pi \end{aligned}$$

לכן $I = \sqrt{2\pi}$.

עבור $t > 0$ נסמן $f_t(x) = e^{-\frac{x^2}{2t}}$ אז

$$\widehat{f_t}(\omega) = \int_{-\infty}^{\infty} e^{-\frac{x^2}{2t}} e^{-2\pi i\omega x} dx$$

ממשפט ההתכנסות הנשלטת של לבג, מותר לגזור מתחת לאינטגרל לפי ω ומקבלים

$$\begin{aligned} \frac{d}{d\omega}\widehat{f_t} &= -2\pi i \int_{-\infty}^{\infty} x \cdot e^{-\frac{x^2}{2t}} e^{-2\pi i\omega x} dx \\ &= 2\pi it \int_{-\infty}^{\infty} \frac{d}{dx}\left(e^{-\frac{x^2}{2t}}\right) e^{-2\pi i\omega x} dx \\ &= 2\pi it \left[\left(e^{-\frac{x^2}{2t}}\right) \cdot e^{-2\pi i\omega x}\right]_{x=-\infty}^{\infty} - 2\pi it \int_{-\infty}^{\infty} e^{-\frac{x^2}{2t}} \frac{d}{dx}\left(e^{-2\pi i\omega x}\right) dx \\ &= 2\pi it \int_{-\infty}^{\infty} 2\pi i\omega e^{-\frac{x^2}{2t}} e^{-2\pi i\omega x} dx \\ &= -4\pi^2 t\omega \int_{-\infty}^{\infty} e^{-\frac{x^2}{2t}} e^{-2\pi i\omega x} dx \\ &= -4\pi^2 t\omega \cdot f_t(\omega) \end{aligned}$$

נשים לב כי

$$\begin{aligned}
\frac{d}{d\omega}\left(e^{2\pi^2\omega^2 t}\widehat{f}_t(\omega)\right) &= 4\pi^2\omega t\cdot e^{2\pi^2\omega^2 t}\cdot\widehat{f}_t(\omega)+e^{2\pi^2\omega^2 t}\cdot\left(\frac{d}{d\omega}\widehat{f}_t\right)(\omega)\\
&= e^{2\pi^2\omega^2 t}\left(4\pi^2\omega t-4\pi^2\omega t\right)f_t(\omega)=0
\end{aligned}$$

מכאן

$$\widehat{f}_t(\omega) = \widehat{f}_t(0)\cdot e^{-2\pi^2\omega^2 t}$$

נחשב

$$\begin{aligned}
\widehat{f}_t(0) &= \int_{-\infty}^{\infty} e^{-\frac{x^2}{2t}}dx\\
\underbrace{}_{x=\sqrt{t}u} &= \int_{-\infty}^{\infty} e^{-\frac{u^2}{2}}\sqrt{t}du\\
&= \sqrt{2\pi t}
\end{aligned}$$

סה"כ קיבלנו

$$\begin{aligned}
f_t(x) &= e^{-\frac{x^2}{2t}}\\
\widehat{f}_t(\omega) &= \sqrt{2\pi t}e^{-2\pi^2\omega^2 t}
\end{aligned}$$

נקח $t=\frac{1}{2\pi}$ ונקבל

$$\begin{aligned}
f(x)=f_{\frac{1}{2\pi}}(x) &= e^{-\pi x^2}\\
\hat{f}(\omega)=\widehat{f_{\frac{1}{2\pi}}}(\omega) &= e^{-\pi\omega^2}
\end{aligned}$$

כלומר $f(x)=\hat{f}(x)$.

4.3 המשוואה הפונקציונלית של פונקציית θ

הגדרה 4.2

$$\theta(x) = \sum_{n=-\infty}^{\infty} e^{-n^2\pi x}$$

נייישם את נוסחת פואסון עבור $f_t(x)=e^{-\frac{x^2}{2t}}$ (כאשר $t>0$) ונקבל

$$\begin{aligned}
\sum_{n=-\infty}^{\infty} e^{-\frac{n^2}{2t}} &= \sum_{n=-\infty}^{\infty} f_t(n)\\
&= \sum_{n=-\infty}^{\infty} \widehat{f}_t(n)\\
&= \sqrt{2\pi t}\sum_{n=-\infty}^{\infty} e^{-2\pi^2 n^2 t}
\end{aligned}$$

נציב $x=2\pi t$ (כלומר $t=\frac{x}{2\pi}$) ואז נקבל

$$\sum_{n=-\infty}^{\infty} e^{-\frac{n^2\pi}{x}} = \sqrt{x}\sum_{n=-\infty}^{\infty} e^{-\pi n^2 x}$$

כלומר $\theta\left(\frac{1}{x}\right)=\sqrt{x}\theta\left(x\right)$ או $\theta\left(x\right)=\frac{1}{\sqrt{x}}\theta\left(\frac{1}{x}\right)$.

4.4 חסמים

עבור $x>0$ מתקיים

$$\frac{\theta\left(x\right)-1}{2} = \sum_{n=1}^{\infty} e^{-n^2\pi x} < \sum_{n=1}^{\infty} e^{-nx} = \frac{e^{-x}}{1-e^{-x}} = \frac{1}{e^x-1}$$

בפרט

1. $\int_1^\infty \frac{\theta(x)-1}{2}x^z dx$ מתכנס לכל $z\in\mathbb{C}$ ומגדיר פונקציה שלמה.
2. $\theta\left(x\right)$ חסום על $x\geq 1$ כי

$$\left|\theta\left(x\right)\right| \leq \underbrace{1+\frac{2}{e-1}}_{C}$$

3. בנוסף עבור $0\leq x\leq 1$ מתקיים

$$\theta\left(x\right) = \frac{1}{\sqrt{x}}\theta\left(\frac{1}{x}\right)\leq\frac{C}{\sqrt{x}}$$

ובפרט $\int_0^1 \theta\left(x\right)x^z\frac{dx}{x}$ ו$\int_0^1 \left(\theta\left(x\right)-1\right)x^z\frac{dx}{x}$ מתכנסים ל$\mathrm{Re}z>\frac{1}{2}$.

5 ההוכחה השנייה של רימן

5.1 טרנספורם מלין

1. תהי φ פונקציה על $(0,\infty)$, אז טרנספורם מלין של φ היא הפונקציה

$$\Phi\left(s\right) = \int_0^\infty \varphi\left(x\right)x^s\frac{dx}{x}$$

כאשר s מרוכב (עבור אותם הsים שהאינטגרל מתכנס).

2. נגדיר f על $\left(-\infty,\infty\right)$ על ידי $f\left(t\right)=\varphi\left(e^t\right)$. קיים טנספורם פוריה

$$\omega \mapsto \hat{f}\left(\omega\right)=\int_{-\infty}^{\infty} f\left(t\right)e^{-it\omega}dt$$

אם ניקח ω מרוכב אז נקבל טרנספורם לפלס

$$s \quad \mapsto \quad \int_0^\infty f(t)\, e^{st} dt$$

(אולי יש e^{-st} בתוך האינטגרל, אבל זה לא כל כך משנה) ואז

$$\begin{aligned} \Phi(s) &= \int_0^\infty \varphi(x)\, x^s \frac{dx}{x} \\ \underbrace{}_{x=e^t} &= \int_{-\infty}^\infty \varphi\left(e^t\right) e^{ts} dt \\ &= \int_{-\infty}^\infty f(t)\, e^{ts} dt \end{aligned}$$

כלומר טרנספורם מלין של φ הוא למעשה טרנספורם לפלס של $f(t) = \varphi\left(e^t\right)$

הערה 5.1 (הסבר נוסף): $x \mapsto x^s$ הם כרקרטים של החבורה $\mathbb{R}_+ = (0,\infty)$ וטרנספורם מלין הוא המשכה אנליטית, $\frac{dx}{x}$ מידת האר.

5.2 הוכחה שנייה של רימן להמשכה מרומורפית של ζ ולמשוואה הפונקציונלית

נתחיל עם $s > 1$ ממשי

$$\begin{aligned} \int_0^\infty e^{-n^2\pi x} \cdot x^{\frac{s}{2}} \frac{dx}{x} &= \int_0^\infty e^{-n^2\pi x} \cdot \frac{\left(n^2\pi x\right)^{\frac{s}{2}}}{\left(n^2\pi\right)^{\frac{s}{2}}} \frac{dx}{x} \\ \underbrace{}_{n^2\pi x = t} &= \int_0^\infty e^{-t} \cdot \frac{t^{\frac{s}{2}}}{\left(n^2\pi\right)^{\frac{s}{2}}} \frac{dt}{t} \\ &= \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \cdot \frac{1}{n^s} \end{aligned}$$

לכן

$$\begin{aligned} \int_0^\infty \left(\theta(x) - 1\right) x^{\frac{s}{2}} \frac{dx}{x} &= 2\int_0^\infty \left(\sum_{n=1}^\infty e^{-n^2\pi x}\right) x^{\frac{s}{2}} dx \\ &= 2\sum_{n=1}^\infty \int_0^\infty e^{-n^2\pi x} x^{\frac{s}{2}} dx \\ &= 2\sum_{n=1}^\infty \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \cdot \frac{1}{n^s} \\ &= 2\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) \end{aligned}$$

כאשר ניתן להחליף את האינטגרל ואת הסכום ממשפט ההתכנסות המונוטונית.

לכן די להוכיח כי לפונקציה $x\mapsto\int_0^\infty(\theta(x)-1)\,x^{\frac{s}{2}}dx$ ($s>1$) יש המשכה מרומורפית, ושהמשכה זו אינווריאנטית לשיקוף $s\mapsto 1-s$.

כעת: עדיין $s>1$ ממשי

$$\begin{aligned}\int_0^1(\theta(x)-1)\,x^{\frac{s}{2}}\frac{dx}{x} &\underbrace{=}_{\substack{y=\frac{1}{x}\\ dx=-\frac{1}{y^2}dy\\ dx=-x^2dy}} \int_1^\infty\left(\theta\left(\frac{1}{y}\right)-1\right)y^{-\frac{s}{2}}y^{-1}dy\\ &= \int_1^\infty\left(\theta\left(\frac{1}{x}\right)-1\right)x^{-\frac{s}{2}}\frac{dy}{y}\\ &= \int_1^\infty\left(\sqrt{x}\theta(x)-1\right)x^{-\frac{s}{2}}\frac{dx}{x}\\ &= \int_1^\infty\left(x^{\frac{1-s}{2}}\theta(x)-x^{-\frac{s}{2}}\right)\frac{dx}{x}\\ &= \int_1^\infty(\theta(x)-1)\,x^{\frac{1-s}{2}}\frac{dx}{x}+\int_1^\infty\left(x^{\frac{1-s}{2}}-x^{-\frac{s}{2}}\right)\frac{dx}{x}\end{aligned}$$

נחשב

$$\begin{aligned}\int_1^\infty\left(x^{\frac{1-s}{2}}-x^{-\frac{s}{2}}\right)\frac{dx}{x} &= \int_1^\infty\left(x^{\frac{1-s}{2}-1}-x^{-\frac{s}{2}-1}\right)dx\\ &= \left[\frac{x^{\frac{1-s}{2}}}{\frac{1-s}{2}}-\frac{x^{-\frac{s}{2}}}{-\frac{s}{2}}\right]_1^\infty\\ &= -\left(\frac{2}{1-s}+\frac{2}{s}\right)\end{aligned}$$

לבסוף ל$s>1$

$$\begin{aligned}2\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \int_0^\infty(\theta(x)-1)\,x^{\frac{s}{2}}\frac{dx}{x}\\ &= \int_0^1(\theta(x)-1)\,x^{\frac{s}{2}}\frac{dx}{x}+\int_1^\infty(\theta(x)-1)\,x^{\frac{s}{2}}\frac{dx}{x}\\ &= \int_1^\infty(\theta(x)-1)\,x^{\frac{1-s}{2}}\frac{dx}{x}+\int_1^\infty\left(x^{\frac{1-s}{2}}-x^{-\frac{s}{2}}\right)\frac{dx}{x}+\int_1^\infty(\theta(x)-1)\,x^{\frac{s}{2}}\frac{dx}{x}\\ &= \int_1^\infty(\theta(x)-1)\left(x^{\frac{1-s}{2}}+x^{\frac{s}{2}}\right)\frac{dx}{x}-\frac{2}{1-s}-\frac{2}{s}\end{aligned}$$

נשים לב כי צד ימין הוא פונקציה מרומורפית האינווריאנטית ל$s\mapsto 1-s$. מכאן מסיקים שיש המשכה מרומורפית לζ ושמתקיימת המשוואה הפונקציונלית הסימטרית

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{(1-s)}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

6 חוגי דדקינד

6.1 אידאלים שבריים בתחומי שלמות

יהי R תחום שלמות ($1 \neq 0$ ואין מחלקי אפס). יהי K שדה המנות של R. בפרט K הוא R־מודול.

טענה 6.1 יהי $K \supseteq I \neq 0$ תת R־מודול של K (כלומר $I \neq 0$ ו־$IR \subseteq I$). התנאים הבאים שקולים:

1. קיים $0 \neq a \in R$ כך ש־$aI \subseteq R$ (ואז aI הוא אידאל של R)
2. קיים $0 \neq a \in K$ כך ש־$aI \subseteq R$ (ואז aI הוא אידאל של R)
3. (במקרה ו־R נתר) I נוצר סופית כ־R־מודול

הוכחה: $1 \Longleftarrow 2$. ברור. נראה $1 \Longrightarrow 2$: נניח כי $a \in K$ מקיים $aI \subseteq R$. נכתוב $a = \frac{\alpha}{\beta}$ כאשר $\alpha, \beta \in R$ ו־$\beta \neq 0$. אז $\frac{\alpha}{\beta} I \subseteq R$ ולכן $\alpha I \subseteq \beta R \subseteq R$.
$1 \Longrightarrow 3$: נניח כי I נוצר סופית כ־R־מודול, אז יש $\frac{\alpha_1}{\beta_1}, \ldots, \frac{\alpha_n}{\beta_n} \in I$ כך שכל איבר $x \in I$ ניתן לכתיבה בצורה

$$x = r_1 \frac{\alpha_1}{\beta_1} + \ldots + r_n \frac{\alpha_n}{\beta_n}$$

ואז $\beta_1 \beta_2 \ldots \beta_n x \in R$ לכל $x \in I$ כלומר $\beta_1 \ldots \beta_n I \subseteq R$.
$3 \Longrightarrow 1$: מתקיים כי יש $a \in R$ כך ש־$aI \subseteq R$. כאמור aI הוא אידאל של R ולכן מאחר ו־R חוג נתר, מתקיים כי aI נוצר סופית. לכן גם I נוצר סופית. ■

הגדרה 6.2 אם $K \supseteq I \neq 0$ תת R־מודול של K המקיים את אחד התנאים השקולים במשפט, נאמר כי I אידאל שברי של R (Fractional ideal).

הערה 6.3 האידאלים השבריים של I של R המקיימים $I \subseteq R$ הם בדיוק האידאלים השונים מ־0 של R ונקראים גם אידאלים שלמים.

נסמן ב־$\mathfrak{F}(R)$ את האידאלים השבריים של R וב־$I(R)$ את האידאלים השלמים של R.

6.1.1 פעולות על אידאלים שבריים

יהיו $I_1, I_2 \subseteq K$ אידאלים שבריים.

1. כפל

$$I_1 I_2 = \left\{ \sum_{\text{finite sum}} a_i b_i \mid a_i \in I_1, b_i \in I_2 \forall i \right\}$$

בפרט $\mathfrak{F}(R)$ ו־$I(R)$ מונואידים עם יחידה R.

2. חיבור

$$I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$$

3. חיתוך: $I_1 \cap I_2$ אידאל שברי.

4. מנה:

$$I_1 : I_2 = \{\alpha \in K \mid \alpha I_2 \subseteq I_1\}$$

ראשית זהו R מודול. הוא שברי: יש $0 \neq d \in K$ כך ש $dI_1 \subseteq R$ ויש $I_2 \ni i_2 \neq 0$ ואם $\alpha \in I_1 : I_2$ אז נובע כי

$$di_2\alpha \in dI_2\alpha \subseteq dI_1 \subseteq R$$

לבסוף $I_1 : I_2 \neq 0$: אכן, יש $0 \neq a \in K$ כך ש$aI_2 \subseteq R$ ואם $0 \neq i_1 \in I_1$ אז $ai_1I_2 \subseteq i_1R \subseteq I_1$. ולכן $I_1 : I_2 \ni ai_1 \neq 0$.

הערה 6.4 מקרה פרטי: אם I אידאל שברי, מוגדר

$$I^{-1} = R : I = \{\alpha \in K \mid \alpha I \subseteq R\}$$

תכונות

(א) אם $I \subseteq R$ (כלומר I שלם) אז $R \subseteq I^{-1}$.

(ב) $II^{-1} \subseteq R$

הגדרה 6.5 אם מתקיים $II^{-1} = R$, אומרים שI הפיך.

הערה 6.6 יהי $I \in \mathfrak{F}(R)$. אז I הפיך אם ורק אם יש $J \in \mathfrak{F}(R)$ כך ש$IJ = R$ ובמקרה זה $J = I^{-1}$.

הוכחה: ראשית נובע כי $J \subseteq I^{-1}$ ולכן $R = IJ \subseteq II^{-1}$. מצד שני ראינו ש$II^{-1} \subseteq R$ ולכן נובע $II^{-1} = R$, כלומר I הפיך. לבסוף, נכפול את $IJ = R$ בI^{-1} ונקבל

$$J = RJ = \left(I^{-1}I\right) J = I^{-1} (IJ) = I^{-1}R = I^{-1}$$

■

הערה 6.7 אם $I_1, \ldots, I_k \in \mathfrak{F}(R)$ אז $I_1 \cdot \ldots \cdot I_k$ הפיך אם ורק אם כל I_i הפיך, ובמקרה זה $(I_1 \cdot \ldots \cdot I_k)^{-1} = I_1^{-1} \cdot \ldots \cdot I_k^{-1}$.

הוכחה: $\Longrightarrow$:

$$\begin{aligned} (I_1 \ldots I_k)\left(I_1^{-1} \ldots I_k^{-1}\right) &= I_1I_1^{-1}I_2I_2^{-1} \ldots I_kI_k^{-1} \\ &= R \cdot R \cdot \ldots R \\ &= R \end{aligned}$$

ומכאן המסקנה (בעזרת ההערה הקודמת)

$\Longleftarrow$: די להוכיח בלי הגבלת הכלליות כי I_1 הפיך, אבל

$$\begin{aligned} (I_1 \ldots I_k)(I_1 \ldots I_k)^{-1} &= R \\ I_1 \left((I_2 \cdot \ldots \cdot I_k)(I_1 \ldots I_k)^{-1}\right) &= R \end{aligned}$$

ומההערה הקודמת נובע כי I_1 הפיך. ■

הערה 6.8 אם $0 \neq a \in K$ אז $aR \in \mathfrak{F}(R)$ (באופן מיידי) ו-aR הפיך ו-$(aR)^{-1} = a^{-1}R$.

הוכחה: מתקיים $(aR)\left(a^{-1}R\right) = R$ ומהערה קודמת נובעת המסקנה. ■

הערה 6.9 אם $I \in \mathfrak{F}(R)$ הפיך ו-$0 \neq a \in K$ אז $aI \in \mathfrak{F}(R)$ הפיך ו-$(aI)^{-1} = a^{-1}I$.

הוכחה: $aI \in \mathfrak{F}(R)$ נובע מכך ש-$aR \in \mathfrak{F}(R)$ וש-$aI = (aR)I$. בנוסף $(aI)^{-1} = (aR)^{-1}I^{-1} = a^{-1}RI^{-1}$. ■

6.2 חוגי דדקינד

הגדרה 6.10 R חוג דדקינד אם:

1. R תחום שלמות
2. R חוג נתר
3. R סגור בשלמות (כלומר אם $x \in K$ הוא מספר אלגברי מעל R, אז $x \in R$)
4. כל אידאל ראשוני $0 \neq P \subseteq R$ הוא מקסימלי

הערה 6.11 בהגדרת תחום דדקינד דרוש גם ש-R אינו שדה.

טענה 6.12 $\mathbb{Z}$ ובאופן כללי כל תחום ראשי (PID) הוא חוג דדקינד.

הוכחה: יהי R תחום ראשי. אז R תחום נתר (באופן מיידי). נוכיח שכל $0 \neq P \subseteq R$ ראשוני הוא מקסימלי. יהי M אידאל עם $P \subseteq M \subsetneqq R$ ונוכיח $P = M$: יש $x, y \in R$ עם $P = xR$ ו-$M = yR$. $x \in P \subseteq M$ ולכן יש $a \in R$ כך ש-$x = ay \in P$. P הוא אידאל ראשוני ולכן $a \in P$ או $y \in P$. אם $a \in P$ אז יש $b \in R$ כך ש-$a = bxw$ ואז מקבלים $x = bxy$ ו-$x \neq 0$ ולכן $by = 1$. מכאן $M = yR = R$ (כי $yR \subseteq R$ ו-$yR \supseteq ybR = R$). סתירה. לכן $a \notin P$ ומכאן $y \in P$ ואז $M = yR \subseteq P$ ולכן $M = P$.

נוכיח ש-R סגור בשלמות: ניתן לעשות זאת בשתי דרכים: הראשונה היא באמצעות העובדה שכל תחום ראשי הוא תחום פריקות יחידה, אך זו הוכחה די ארוכה. נציג הוכחה ישירה במקום: יהי $u \in K$ שלם מעל R (K שדה המנות של R). אנו צריכים להוכיח כי $u \in R$. ובכן u מקיים משוואה מהצורה

$$u^n + c_{n-1}u^{n-1} + \ldots + c_0 \quad = \quad 0$$

עם $n \geq 1$ ו-$c_i \in R$ לכל $0 \leq i \leq n-1$.
נסמן

$$N \quad = \quad Ru^{n-1} + \ldots + Ru + R \subseteq K$$

אז N הוא מודול נוצר סופית. נכתוב $u = \frac{r}{s}$. אז ע"י הכפלה ב-s^{n-1} נקבל כי $s^{n-1}N$ הוא אידאל ב-R ולכן זהו אידאל ראשי, לכן קיים $z \in K$ כך ש-$N = zR$. מאחר ו-u מקיים את המשוואה הפולינומיאלית הנ"ל, N סגור בכפל ב-u ולכן $N^2 = N$. בפרט $z^2 \in N = zR$ ולכן קיים $r \in R$ כך ש-$z^2 = zr$. $z \neq 0$ ולכן $z = r$ ולבסוף $u \in N = zR = rR \subseteq R$. ■

6.3 משפט פירוק אידאלים

יהי R חוג דדקינד.

למה 6.13 לכל אידאל שלם $0 \neq I \subseteq R$ קיימים אידאלים ראשוניים השונים מאפס $(P_1, \ldots, P_n)$ עם $n \geq 1$ כך ש $P_1 \ldots P_n \subseteq I$.

הוכחה: אם הלמה לא נכונה, קיים אידאל $I \neq 0$ מקסימלי ביחס להכלה מתוך כל אלה שעבורם הלמה לא נכונה. (כי R חוג נתר)
I לא ראשוני (כי הלמה נכונה לכל ראשוני) ולכן יש $a, b \notin I$ כך ש$ab \in I$. מתקיים $I \subsetneqq I_1 = I + aR$ ו$I \subsetneqq I_2 = I + bR$ ומתקיים $I_1 \cdot I_2 \subseteq I$. מאחר ו$I$ מקסימלי ביחס להכלה מבין כל האידאלים שהלמה אינה נכונה עבורם, הלמה נכונה עבור I_1 וI_2 ולכן $I_1 I_2 \subseteq I$ ולכן לI. סתירה. ■

למה 6.14 אם $0 \neq P \subseteq R$ ראשוני אז $R \subsetneqq P^{-1}$.

הוכחה: ברור ש$R \subseteq P^{-1}$ (כי $PR \subseteq P \subseteq R$) ולכן צריך להוכיח כי $R \neq P^{-1}$.
יהי $0 \neq a \in P$ ויהיו $P_1, \ldots, P_n$ ראשוניים השונים מאפס כך ש $P_1 \cdot \ldots \cdot P_n \subseteq aR \subseteq P$.
נבחר $P_1, \ldots, P_n$ כנ"ל עם n מינימלי. ($n = 0$ גורר $P \subseteq aR \subseteq R$ כלומר $P = R$ וזו סתירה. לכן $n \geq 1$)
מאחר שP ראשוני, יש i עם $P_i \subseteq P$, ולכן $P = P_i$ (כי בחוג דדקינד אידאל ראשוני הוא מקסימלי). נניח בלי הגבלת הכלליות כי $P_1 = P$.
כעת ממינימליות n מתקיים כי $P_2 \cdot \ldots \cdot P_n \not\subseteq aR$ ולכן יש $b \in P_2 \cdot \ldots \cdot P_n$ עם $b \notin aR$, כלומר $a^{-1}b \notin R$. נטען כי $a^{-1}b \in P^{-1}$: אכן

$$Pb \quad \subseteq \quad P_1 P_2 \ldots P_n \subseteq aR$$

ולכן

$$\left(a^{-1}b\right) P \quad \subseteq \quad R$$

ומכאן $a^{-1}b \in P^{-1}$ ו$a^{-1}b \notin R$ כנדרש. ■

למה 6.15 יהי $0 \neq P \subseteq R$ אידאל ראשוני ו$I \subseteq K$ אידאל שברי, אז $I \subsetneqq IP^{-1}$.

הוכחה: $R \subseteq P^{-1}$ ולכן $I \subseteq IP^{-1}$ ולכן כמו קודם נותר להוכיח כי $I \neq IP^{-1}$.
נניח בשלילה כי $I = IP^{-1}$. יהיו $x_1, \ldots, x_n$ יוצרים של הR-מודול I מעל R. (יש כאלה, כי קיים $a \in R$ כך ש$aI \subseteq R$ ואז aI אידאל של R ומכיוון שאנו בחוג נתר, הוא נוצר סופית, ואז גם I נוצר סופית).
יהי $\alpha \in P^{-1}$ כלשהו, אז $\alpha x_i \in P^{-1} I = I$ לכל $1 \leq i \leq n$. לכן יש $c_{ij} \in R$ כך ש

$$\alpha x_i \quad = \quad \sum_{j=1}^{n} c_{ij} x_j$$

לכל i, כלומר

$$\begin{pmatrix} \alpha - c_{11} & -c_{12} & \ldots & -c_{1n} \\ -c_{21} & \alpha - c_{22} & \ldots & -c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -c_{n1} & -c_{n2} & \ldots & \alpha - c_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad = \quad 0$$

נכפיל בAdjoint ונקבל

$$\det\left(\left(\alpha\delta_{ij}-c_{ij}\right)_{i,j=1}^{n}\right)\cdot x_j \quad = \quad 0$$

נבחר $x_j \neq 0$ (יש כזה כי $I \neq 0$) ונקבל $\det\left(\left(\alpha\delta_{ij}-c_{ij}\right)_{i,j=1}^{n}\right)=0$. מכאן α מקיים משוואה מהצורה

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 \quad = \quad 0$$

כאשר $a_k \in R$ לכל $0 \leq k \leq n-1$. לכן $\alpha \in R$. מכאן הראנו $P^{-1} \subseteq R$ ולכן $P^{-1}=R$, בסתירה ללמה הקודמת. ■

מסקנה 6.16 אם $R \supseteq P \neq 0$ אידאל ראשוני אז $PP^{-1}=R$, כלומר כל אידאל ראשוני הוא הפיך.

הוכחה: מתקיים מהלמה הקודמת

$$P \quad \subsetneqq PP^{-1} \quad \subseteq R$$

אבל P אידאל ראשוני בחוג דדקינד ולכן מקסימלי וPP^{-1} אידאל המכיל אותו ממש. לכן $PP^{-1}=R$. ■

משפט 6.17 יהי R חוג דדקינד, אז:

1. כל אידאל שברי הוא הפיך.
2. לכל אידאל שלם $R \supseteq I \neq \{0\}$ יש פירוק $I=P_1\cdot\ldots\cdot P_n$ כאשר לכל $1 \leq i \leq n$ מתקיים כי $0 \neq P_i$ אידאל ראשוני, ופירוק זה הוא יחיד עד כדי סדר הגורמים.

הערה 6.18 אם $I=R$ אז נקח $n=0$ (הפירוק הריק).

הוכחה: קיום הפירוק: אם הקיום לא היה נכון, אז היה אידאל $R \supsetneqq I \neq 0$ מקסימלי (ביחס להכלה) מבין אלה ללא פירוק. אז $I \neq R$ (כי לR הפירוק הריק) ולכן יש אידאל מקסימלי M (ולכן ראשוני) המקיים $I \subseteq M$. מהלמה הקודמת מתקיים

$$I \quad \subsetneqq IM^{-1} \quad \subseteq MM^{-1} \subseteq R$$

ולכן IM^{-1} אידאל המכיל ממש את I ולכן יש לIM^{-1} פירוק

$$IM^{-1} \quad = \quad P_1\cdot\ldots\cdot P_k$$

כאשר $P_1,\ldots,P_k$ אידאלים ראשוניים. מאחר וM ראשוני, נובע כי $MM^{-1}=R$ ולכן

$$I \quad = \quad IR=IM^{-1}M=P_1\cdot\ldots\cdot P_k\cdot M$$

פירוק של I.

הפיכות: מקיום הפירוק נובע שכל אידאל שלם הפיך. אם J אידאל שברי, יש $c\in K^{\times}$ ואידאל שלם I עם $J=cI$ ולכן J הפיך עם $J^{-1}=c^{-1}I^{-1}$.

יחידות הפירוק: נובעת מהלמה (היותר כללית) הבאה:

למה 6.19 יהי R תחום שלמות עם $0 \neq I \subseteq R$ אידאל שלם הפיך. אם יש לI פירוק $I = P_1 \cdot \ldots \cdot P_n$ כאשר $P_i \neq 0$ אידאל ראשוני לכל $1 \leq i \leq n$, אז פירוק זה יחיד עד כדי סדר.

הוכחה: נסתכל על פירוק כלשהו $I = Q_1 \cdot \ldots \cdot Q_l$ (כאשר $0 \neq Q_j \subseteq R$ ראשוני לכל $1 \leq j \leq l$), ונוכיח הוא כמו בלמה.
מתקיים כי $Q_1 \cdot \ldots \cdot Q_l = P_1 \cdot \ldots \cdot P_n \subseteq P_1$ ולכן מתקיים $Q_j \subseteq P_1$ לאיזשהו $1 \leq j \leq l$.
ניתן להניח בלי הגבלת הכלליות (ע"י שינוי הסדר) כי $Q_1 \subseteq P_1$. כל P_i וכל Q_j הפיך (כי I הפיך). נוכיח כי $P_1 = Q_1$ ואז ע"י כפל ב$Q_1^{-1} = P_1^{-1}$ ושימוש בהפיכות נקבל $P_2 \cdot \ldots \cdot P_n = Q_2 \cdot \ldots \cdot Q_l$ ונמשיך באינדוקציה.
נסתכל על $T = P_1^{-1}Q_1$ אז מאחר ו$Q_1 \subseteq P_1$ מתקיים כי $T \subseteq P_1^{-1}P_1 = R$ ולכן T אידאל שלם. מתקיים $TP_1 = Q_1$ (כי P_1 הפיך). בפרט T הפיך (כי Q_1 הפיך). Q_1 ראשוני ולכן מתוך $TP_1 = Q_1$ נובע כי $P_1 \subseteq Q_1$ או $T \subseteq Q_1$. אם $P_1 \subseteq Q_1$, אז סיימנו. אחרת $T \subseteq Q_1$ ואז $T \subseteq TP_1$ וע"י כפל בT^{-1} (T הוא כאמור הפיך) נקבל $R = T^{-1}T \subseteq T^{-1}TP_1$ כלומר $R \subseteq P_1$, כלומר $R = P_1$. סתירה. ■

■

הערה 6.20 קיימות פונקציות יחידות

$$\nu_P(\cdot) : \{\text{integral ideals}\} \quad \longrightarrow \quad \{0, 1, 2, 3, \ldots\}$$

(כאשר $0 \neq P \subseteq R$ ראשוני) כך שלכל אידאל שלם $0 \neq I \subseteq R$ מתקיים $\nu_P(I) = 0$, כמעט לכל P (כלומר פרט אולי למספר סופי) ו

$$I \quad = \quad \prod_{\substack{0 \neq P \subseteq R \\ P \text{ is prime}}} P^{\nu_P(I)}$$

הערה 6.21 באשר לפירוק של אידאל שלם:

$$I \quad = \quad P_1^{n_1} \cdot \ldots \cdot P_l^{n_l}$$

(כאשר $P_1, \ldots, P_l$ שונים זה מזה ו$n_i > 0$ לכל i)
עבור $0 \neq P \subseteq R$ מתקיים $I \subseteq P \iff$ יש i כך ש$P_i = P$.

הוכחה: $\Longleftarrow$: מיידי.
$\Longrightarrow$: יש i כך ש$P_i \subseteq P$ ולכן $P = P_i$ ממקסימליות. ■

מסקנה 6.22 $I \subseteq P \iff \nu_P(I) > 0$ (כאשר $0 \neq P \subseteq R$ אידאל ראשוני וI אידאל שלם).

מסקנה 6.23 כל אידאל שלם השונה מאפס מוכל במספר סופי של אידאלים ראשוניים.

מסקנה 6.24 $I_1 : I_2 = I_1 \cdot I_2^{-1}$ (כאשר $I_1, I_2 \subseteq K$ אידאלים שבריים)

הוכחה: יהי $x \in K$ אז $x \in I_1 \cdot I_2^{-1} \iff xI_2 \subseteq I_1 I_2^{-1} I_2 = I_1 \iff x \in I_1 : I_2$. ■

מסקנה 6.25 קבוצת האידאלים השבריים היא חבורה חילופית עם יחידה R וההופכי של כל I הוא $I^{-1}=\{\alpha\in K \mid \alpha I\subseteq R\}$. בפרט $I=\left(I^{-1}\right)^{-1}$. (כאשר I אידאל שברי)

מסקנה 6.26 "להכפיל זה לחלק": $J\subseteq J' \iff$ קיים אידאל שלם I כך ש $J=J'I$ (כאשר J,J' אידאלים שבריים).

הוכחה: $\Longrightarrow$: $J=J'I\subseteq J'R=J'$
$\Longleftarrow$: נקח $I=J\left(J'\right)^{-1}$ אז $IJ'=J$ ומתקיים $I=J\left(J'\right)^{-1}\subseteq J'\left(J'\right)^{-1}=R$. ■

הערה 6.27 כל אידאל שברי הוא מנה של שני אידאלים שלמים.

הוכחה: אכן, אם J שברי, יש $c\in R^{\times}$ כך ש $I=cJ$ אידאל שלם ואז $J=c^{-1}I=(cR)^{-1}I$. ■

משפט 6.28 לכל אידאל שברי יש $n\geq 0$ ו$0\neq P_1,P_2,\ldots,P_n\subseteq R$ ראשוניים שונים ו$0\neq \nu_i\in\mathbb{Z}$ כך ש $I=\prod_{i=1}^{n}P_i^{\nu_i}$ ופירוק זה יחיד עד כדי הסדר.

הוכחה: <u>קיום:</u> מיידי מההערה.
<u>יחידות:</u> די להוכיח כי אם $P_1^{n_1}\cdot\ldots\cdot P_k^{n_k}=R$ עם $P_1,\ldots,P_k$ אידאלים ראשוניים השונים מ0 השונים מזה, עם $n_i\in\mathbb{Z}$ אז $n_i=0$ (לכל $1\leq i\leq k$)..
אפשר להניח כי

$$n_1\leq n_2\leq\quad\ldots\quad\leq n_t\leq n_{t+1}\leq\ldots\leq n_k$$

ונקבל

$$P_1^{n_1}\cdot\ldots\cdot P_k^{n_k}\quad=\quad P_{t+1}^{n_{t+1}}\cdot\ldots\cdot P_k^{n_k}$$

פירוקים שונים של אותו אידאל שלם. מיחידות פירוק אידאלים שלמים נסיק כי $n_i=0$ לכל $1\leq i\leq k$. ■

מסקנה 6.29 אוסף האידאלים השבריים הוא חבורה חופשית עם בסיס המורכב מקבוצת האידאלים הראשוניים השונים מ0. כמו, כן, לפונקציה ν_P יש הרחבה יחידה ל

$$\nu_P:\{\text{fractional ideals}\}\quad\longrightarrow\quad\mathbb{Z}$$

כך ש$\nu_P(J)=0$ כמעט לכל p (כאשר J שברי) ומתקיים

$$J\quad=\quad\prod_P P^{\nu_P(J)}$$

ו

$$J^{-1}\quad=\quad\prod_P P^{-\nu_P(J)}$$

ולכן $\nu_P\left(J^{-1}\right)=-\nu_P(J)$.
מתקיימות התכונות הבאות:

1. הכלה: אם I שברי אז $I \subseteq R$ (כלומר I שלם) $\iff$ $0 \geq \nu_P(I)$ לכל $P \neq 0$ ראשוני.

הוכחה: $\Longleftarrow$ נובע ממשפט הפירוק (עד כדי יחידות).
$\Longrightarrow$ טריוואלי. ■

2. $\nu_P(I \cdot I_1) = \nu_P(I) + \nu_P(I_1)$ - מיידי מיחידות הפירוק.

3. $I \subseteq I_1 \iff \nu_P(I) \geq \nu_P(I_1)$ לכל P ראשוני (כאשר I ו-I_1 שבריים).

הוכחה: $I \subseteq I_1 \iff I \cdot I_1^{-1} \subseteq R \iff 0 \geq \nu_P(I) - \nu_P(I_1) = \nu_P\left(I \cdot I_1^{-1}\right)$ ■

מסקנה 6.30 אם $I \subseteq R$ אידאל שלם אז

$$\nu_P(I) = \max\{n \mid I \subseteq P^n\}$$

בדיקה: $I \subseteq P^n \iff \nu_P(I) \geq \nu_P(P^n)$ (כי עבור $P' \neq P$ מתקיים אוטומטית $\nu_{P'}(P) = 0 \leq \nu_{P'}(I)$) ולכן

$$\begin{aligned}\nu_P(I) &= \max\{n \mid \nu_P(I) \geq n\} \\ &= \max\{n \mid I \subseteq P^n\}\end{aligned}$$

מסקנה 6.31 $\nu_P(I_1 + \ldots + I_k) = \min\{\nu_P(I_1), \ldots, \nu_P(I_k)\}$
(כאשר $I_1, \ldots, I_k$ שבריים).

הוכחה: מתקיים כי $I_1 + \ldots + I_k$ הוא האידאל השברי הקטן ביותר המכיל את $I_1, \ldots, I_k$.
מצד שני הפונקציה $P \mapsto \min\{\nu_P(I_j) \mid 1 \leq j \leq k\}$ היא הפונקציה הגדולה ביותר הקטנה או שווה לכל אחת מבין $P \mapsto \nu_P(I_j)$. ■

מסקנה 6.32 $\nu_P(I_1 \cap \ldots \cap I_k) = \max\{\nu_P(I_1), \ldots, \nu_P(I_K)\}$
(כאשר $I_1, \ldots, I_k$ שבריים) - הוכחה דומה.

מסקנה 6.33 אם $n_1, \ldots, n_k \geq 0$ ו-$P_1, \ldots, P_k$ ראשוניים השונים זה מזה, אז

$$P_1^{n_1} \cdot \ldots \cdot P_k^{n_k} = P_1^{n_1} \cap \ldots \cap P_k^{n_k}$$

אכן: $\nu_P\left(P_1^{n_1} \cdot \ldots \cdot P_k^{n_k}\right) = \sum_{i=1}^k \nu_P\left(P_i^{n_i}\right)$ ועבור הפונקציות

$$\begin{aligned}&\nu_\cdot\left(P_j^{n_j}\right) \\ &\quad P \mapsto \nu_P\left(P_j^{n_j}\right)\end{aligned}$$

מתקיים כי הסכום = המקסימום.

6.4 איפיון חוגי דדקינד

טענה 6.34 יהי R חוג שאינו שדה. התנאים הבאים שקולים:

1. R הוא חוג דדקינד
2. כל אידאל שברי בR הוא הפיך

הוכחה: $1 \Longleftarrow 2$: ראינו.
$2 \Longleftarrow 1$:

- R נתר: יהי $I \subseteq R$ אידאל. מאחר ש$II^{-1}=R$, יש $n \geq 1$ ו$a_i \in I$ ו$b_i \in I^{-1}$ עם $\sum_{i=1}^{n} a_i b_i = 1$. לכל $x \in I$ מתקיים $xb_i \in R$, ולכן

$$x = x \cdot 1 = \sum_{i=1}^{n} a_i \left(x b_i\right) \in \sum_{i=1}^{n} a_i R$$

ומכאן I נוצר ע"י $a_1, \ldots, a_n$.

- R סגור בשלמות: יהי $x \in K$ שלם מעל R המקיים

$$x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$$

כאשר $a_i \in R$ לכל $1 \leq i \leq n$. נסמן

$$J = x^{n-1} R + \ldots + xR + R$$

אז $J \subseteq K$ שברי ולכן $J^{-1}J = R$. אבל מאחר וx מקיים את הפולינומיאלית המשוואה הנ"ל, נובע כי J חוג ומכאן $J^2 = J$ ולכן

$$J = JR = J\left(JJ^{-1}\right) = J^2 J^{-1} = JJ^{-1} = R$$

ולכן $x \in J = R$ כנדרש.

- כל אידאל ראשוני $0 \neq$ הוא מקסימלי: יהי $0 \neq P \subseteq R$ ראשוני. יהי $M \subseteq R$ אידאל מקסימלי המכיל את P. מתקיים $P \subseteq M \subsetneqq R$. צ"ל $P = M$. נוכיח זאת בדרך השלילה: נניח כי $P \neq M$, כלומר $P \subsetneqq M$. מתקיים $PM^{-1} \subseteq MM^{-1} = R$ ולכן PM^{-1} הוא אידאל שלם ומתקיים $P = \left(PM^{-1}\right)M$. P הוא ראשוני ו$M \subsetneqq P$ ולכן $PM^{-1} \subseteq P$. לכן

$$M^{-1} = P^{-1}PM^{-1} = P^{-1}\left(PM^{-1}\right) \subseteq P^{-1}P = R$$

אבל $R \subseteq M^{-1}$ (כי $MR \subseteq M \subseteq R$) ולכן קיבלנו $M^{-1} = R$ ומכאן $M = MR = MM^{-1} = R$. סתירה.

■

טענה 6.35 יהי R תחום שלמות שאינו שדה. התנאים הבאים שקולים:

1. R דדקינד

2. כל אידאל שלם בR הוא מכפלה של אידאלים ראשוניים.

הוכחה: $1 \Longleftarrow 2$: ראינו.

$2 \Longleftarrow 1$: די להוכיח כי אידאל ראשוני השונה מ0 הוא הפיך: אכן מכיוון שכל אידאל שלם ניתן לכתיבה כמכפלה של אידאלים ראשוניים נובע כי כל אידאל שלם הוא הפיך, ומאחר וכל אידאל שברי J הוא מהצורה $J = cI$ כאשר $c \in K$ וI שלם, נובע כי J הפיך. ראינו שאם כל אידאל שברי הוא הפיך, אז R חוג דדקינד.

נוכיח בהמשך כי כל אידאל ראשוני השונה מ0 והפיך הוא מקסימלי. נניח שהוכחנו זאת ונוכיח כי אידאל ראשוני השונה מ0 הוא הפיך. יהי $0 \neq P \subseteq R$ ראשוני, נראה כי P הפיך. יהי $0 \neq b \in P$. אז $bR = P_1 P_2 \cdot \dots \cdot P_n$ הפיך (כי $b^{-1}R$ הוא ההופכי שלו) כאשר $P_j \neq 0$ ראשוני לכל $1 \leq j \leq n$. מאחר ו $P \supseteq bR = P_1 \cdot P_2 \cdot \ldots \cdot P_n$, נובע כי יש i כך ש$P \supseteq P_i$. P_i הפיך כי bR הפיך ו $bR = P_1 \cdot P_2 \cdot \dots \cdot P_n$. מאחר ו$P_i \neq 0$ ראשוני והפיך נובע כי P_i מקסימלי ולכן $P = P_i$, וP הפיך. כנדרש.

נותר להראות כי כל אידאל ראשוני השונה מ0 והפיך הוא מקסימלי: יהי $0 \neq P \subseteq R$ אידאל ראשוני הפיך. נוכיח כי P מקסימלי. די להוכיח כי לכל $a \in R \setminus P$ מתקיים $aR + P = R$. נוכיח זאת על דרך השלילה: יהי $a \in R \setminus P$ כך ש$aR + P \neq R$. לפי ההנחה יש ל$aR + P$ פירוק $aR + P = P_1 \cdot \dots \cdot P_m$ עם $0 \neq P_i \subseteq R$ ראשוניים ו$m \geq 1$ (אחרת $aR + P = R$). בנוסף $P_i \supseteq aR + P \supseteq P$ ולכן $P_i \supseteq P$ ומתקיים גם כי $P_i \supsetneqq P$ לכל $1 \leq i \leq m$ - כי אילו $P = P_i$ היינו מסיקים $P = P_i \supseteq aR + P = P$ ומכאן $a \in P$, סתירה.

באופן דומה מתקיים כי $a^2 \notin P$ (כי P ראשוני) ו$a^2 R + P \neq R$ (כי $aR + P \neq R$). לכן יש פירוק $a^2 R + P = Q_1 \cdot \dots \cdot Q_n$ עם $n \geq 1$ ו$0 \neq Q_j \subseteq$ ו$P \supsetneqq$ Q_j לכל j. נעבור לתחום $\overline{R} = R/P$ ונסמן את העתקת המנה

$$\begin{array}{ccc} R & \longrightarrow & \overline{R} \\ x & \mapsto & x + P = \overline{x} \end{array}$$

אז $\overline{P_i} \subseteq \overline{R}$ ו$\overline{Q_j} \subseteq \overline{R}$ אידאלים ראשוניים השונים מ0 וכמו כן יש פירוקים

$$\begin{aligned} \overline{a}\overline{R} &= \overline{P_1} \cdot \ldots \cdot \overline{P_m} \\ \overline{a}^2 \overline{R} &= \overline{Q_1} \cdot \dots \cdot \overline{Q_n} \end{aligned}$$

ומהראשון

$$\overline{a}^2 R \;=\; \overline{P_1}^2 \cdot \dots \cdot \overline{P_m}^2$$

$\overline{a}^2 R$ הוא אידאל הפיך ולכן מלמה שהוכחנו נובע ששני הפירוקים האחרונים שווים עד כדי סדר. כלומר הסדרות $\overline{P_1}, \overline{P_1}, \ldots, \overline{P_m}, \overline{P_m}$ ו $\overline{Q_1}, \ldots, \overline{Q_n}$ זהות כולל ריבויים. לכן הסדרות $P_1, P_1, \ldots, P_m, P_m$ ו $Q_1, \ldots, Q_n$ זהות עד כדי סדר ומכאן:

$$(aR + P)^2 \;=\; P_1^2 \ldots P_m^2 = Q_1 \cdot \dots \cdot Q_n = a^2 R + P$$

לכן

$$P \;\subseteq\; a^2 R + P = (aR + P)^2 \subseteq aR + P^2$$

מכאן $P \subseteq (aR \cap P) + P^2$. אבל P ראשוני ו$a \notin P$ ולכן $aR \cap P = aP$. מכאן $P \subseteq aP + P^2 \subseteq P$ ולכן $P = aP + P^2 = (aR + P)\,P$. אבל P הפיך וע"י כפל בP^{-1} מקבלים $aR + P = R$. סתירה. ■

6.5 חוג הערכה דיסקרטיים

הגדרה 6.36 חוג R הוא חוג הערכה דיסקרטית (DVR - Discrete Valuation Ring) אם R תחום ראשי (ובפרט נתר) ובעל אידאל ראשוני יחיד. (R אינו שדה)

הערה 6.37 כל DVR הוא דדקינד (כי הוא PID שאינו שדה).

הערה 6.38 בכל חוג $R^{\times}$ = האיברים ההפיכים. אם R הוא DVR בעל אידאל ראשוני יחיד P, אז $R^{\times} = R \setminus P$.

למה 6.39 יהי R חוג הערכה דיסקרטית ונסמן $0 \neq P \subsetneqq R$ את האידאל הראשוני היחיד. אז $\bigcap_{n=1}^{\infty} P^n = 0$ ובפרט $P^2 \subsetneqq P$.

הוכחה: יהי π יוצר של P (כלומר $P = \pi R$). נסמן $I = \bigcap_{n=1}^{\infty} P^n$ ונניח $I \neq 0$. אז יש $0 \neq y \notin R^{\times}$ כך ש$I = yR$. כעת $I \subseteq P = \pi R$ ולכן יש $a \in R$ כך ש$y = a\pi$. לכל $n \geq 2$ מתקיים

$$a\pi = y \quad \in \quad I = \bigcap_{k=1}^{\infty} P^k \subseteq P^n = \pi^n R$$

ולכן $a \in \pi^{n-1}R = P^{n-1}$. מכאן $a \in \bigcap_{n=1}^{\infty} P^n$ כלומר $a \in I = yR$ ויש $b \in R$ כך ש$a = yb$. בסה"כ קיבלנו $y = a\pi = yb\pi$ ולכן מאחר ו$y \neq 0$ נקבל $b\pi = 1$ ולכן

$$P \quad = \quad \pi R = R$$

סתירה.

זה גם מראה כי $P^2 \neq P$ כי אחרת $P^2 = P$ ואז $\bigcap_{k=1}^{\infty} P^k = P$. ■

6.5.1 פירוק איברים בתחום הערכה דיסקרטית

טענה 6.40 יהי (R, P) תחום הערכה דיסקרטית ויהי K שדה המנות. יהי π יוצר של P. אז לכל $x \in K^{\times}$ יש פירוק יחיד $x = \pi^n u$ עם n שלם ו$u \in R^{\times}$. לבסוף $0 \neq x \in R \iff n \geq 0$.

הוכחה: <u>קיום:</u> מאחר וK שדה המנות של R, אפשר להניח $0 \neq x \in R$, ואז ל$0 \neq x \in K$ כללי יש הצגה כנ"ל כמנה של שני איברים בR עם הצגות כנ"ל. לאור הלמה הקודמת, יש $n \geq 0$ כך ש$x \in P^n \setminus P^{n+1}$. מאחר ש$P^n = \pi^n R$ יש $u \in R$ כך ש$x = \pi^n u$. אילו $u \in P$ היינו מקבלים $x = \pi^n u \in P^{n+1}$ סתירה. לכן $u \notin P$ ולכן $u \in R^{\times}$.

<u>יחידות:</u> נניח כי $\pi^m u = \pi^n v$ ל$u, v \in R^{\times}$. נניח בלי הגבלת הכלליות $n > m$. נובע כי $1 = \pi^{m-n} uv^{-1} \in P$. סתירה.

לבסוף - ראינו כי אם $0 \neq x \in R$ אז $n \geq 0$, ומצד שני ברור כי אם $n \geq 0$ אז $0 \neq x \in R$. ■

מסקנה 6.41 בפירוק $x = \pi^n u$ לעיל מתקיים $n = \nu_P(xR)$ כי $P^{\nu_P(xR)} = xR = \pi^n uR = \pi^n R = P^n$.

מסקנה 6.42 האידאלים השבריים של R הם $P^n = \pi^n R$ ל$n \in \mathbb{Z}$ ו

$$\dots \supsetneqq P^{-2} \supsetneqq P^{-1} \quad \supsetneqq \quad R \supsetneqq P \supsetneqq P^2 \supsetneqq \dots$$

מסקנה 6.43 יהי $0 \neq z \in R$ אז

$$z \in P \setminus P^2 \quad \Longleftrightarrow \quad P = zR$$

מסקנה 6.44 R הוא חוג הערכה בK במובן הבא: יהי $x \in K^\times$ אז $x \in R$ או $x^{-1} \in R$.

מסקנה 6.45 מקסימליות: יהי R חוג DVR, K שדה המנות של R וR' חוג כך ש $R \subsetneqq K \supseteq R'$ אז $R' = K$.

הוכחה: יהי $x \in R' \setminus R$. נכתוב $x = \pi^n u$ עם $u \in R^\times \subseteq (R')^\times$, אז $n \leq -1$. על ידי כפל ב $\pi^{-n-1}u^{-1} \in R \subseteq R'$ נקבל

$$\pi^{-1} = \left(\pi^{-n-1}u^{-1}\right)(\pi^n u) \quad \in \quad R'$$

ולבסוף שוב ע"י הפירוק נובע כי $K \supseteq R'$ ומכאן $R' = K$. ■

טענה 6.46 יהי R חוג. אז R חוג DVR $\Longleftrightarrow$ R חוג דדקינד עם אידאל ראשוני $0 \neq$ יחיד.

הוכחה: ראינו את הכיוון $\Longleftarrow$.

$\Longrightarrow$: נניח כי R דדקינד עם אידאל ראשוני $0 \neq$ יחיד. די להוכיח שR ראשי. מפירוק אידאלים בחוג דדקינד, $P^2 \neq P$. יהי $\pi \in P \setminus P^2$ אז $\pi R = P$ (כי $0 \neq \pi R \subseteq P$ אידאל ולכן ניתן לכתיבה ע"י $\pi R = P^k$ ו$k \leq 1$ כי $\pi \notin P^2 \supseteq P^3 \supseteq \dots$), ולכן P ראשי. לבסוף כל אידאל שלם הוא חזקה של P ולכן כל אידאל כזה הוא ראשי, ומכאן R הוא חוג ראשי. ■

7 מיקום בחוגי דדקינד

7.1 מיקום תחומים כלליים

יהי R תחום.

הגדרה 7.1 קבוצה כפלית בR היא תת־קבוצה $S \subseteq R$ כך ש$1 \in S$, $0 \notin S$ ו$\Longleftarrow$ $s_1 s_2 \in S$ $s_1, s_2 \in S$.

יהי K שדה המנות של R. לכל אידאל שברי $I \subseteq K$ של R נסמן

$$I_S \quad = \quad \left\{ \frac{i}{s} \mid i \in I, s \in S \right\}$$

ובפרט

$$R_S \quad = \quad \left\{ \frac{a}{s} \mid a \in R, s \in S \right\}$$

ואז $K \supseteq R \subseteq R$ ולכל $I \in \mathfrak{F}(R)$ מתקיים $I_S \in \mathfrak{F}(R_S)$.

טענה 7.2 תכונות מיידיות:

1. $I_S = I \cdot R_S$
2. $(I_1 + I_2)_S = (I_1)_S + (I_2)_S$
3. אם $c \in K^\times$ אז $(c \cdot I)_S = c \cdot I_S$
4. $(I_1 I_2)_S = (I_1)_S (I_2)_S$

מסקנה 7.3 קיבלנו הומורפיזמים של מונואידים

$$\begin{aligned} \alpha : \mathfrak{F}(R) &\to \mathfrak{F}(R_S) \\ I &\mapsto I_S \end{aligned}$$

$$\begin{aligned} \alpha' : I(R) &\to I(R_S) \\ I &\mapsto I_S \end{aligned}$$

טענה 7.4 יהי $0 \neq J \subseteq R_S$ אידאל שלם, אז $J = (J \cap R)_S$, ובפרט $J \cap R \subseteq R$ אידאל שלם.

הוכחה: ברור ש

$$(J \cap R)_S = (J \cap R) \cdot R_S \subseteq J$$

מצד שני, יהי $0 \neq \frac{r}{s} \in J$ כאשר $r \in R$ ו$s \in S$ אז

$$\frac{r}{1} = \frac{r}{s} \cdot \frac{s}{1} \in J \cap R$$

ומתקיים

$$\frac{r}{s} = \frac{r}{1} \cdot \frac{1}{s} \in (J \cap R) \cdot R_S = (J \cap R)_S$$

■

הערה 7.5 נובע כי אם $0 \neq Q \subseteq R_S$ אידאל ראשוני אז $Q \cap R \subseteq R$ ראשוני ושונה מאפס.

מסקנה 7.6 α וα' הן על.

הוכחה: α' על נובע מהטענה הקודמת. α על נובע מהפיכת כל אידאל שברי לשלם ע"י כפל באיבר מ K. ■

מסקנה 7.7 (פעולה על I^{-1}): יהי R תחום ו$I \in \mathfrak{F}(R)$ אידאל שברי. אם I נוצר סופית כR מודול, אז

$$\left(I^{-1}\right)_S = (I_S)^{-1}$$

הוכחה: יהי $x = \frac{a}{s} \in \left(I^{-1}\right)_S$, עם $a \in I^{-1}$, אז $aI \subseteq R$ ולכן

$$xI_S = \frac{a}{s}I_S = \frac{a}{s}IR_S \subseteq R_S$$

ולכן $x \in (I_S)^{-1}$.

בכיוון ההפוך, יהיו $t_1, \ldots, t_n$ יוצרים של I מעל R. יהי $y \in (I_S)^{-1}$. אז לכל i מתקיים

$$yt_i \in (I_S)^{-1} I \subseteq (I_S)^{-1} I_S \subseteq R_S$$

ולכן קיים $s_i \in S$ כך ש $yt_is_i \in R$. נסמן $s = s_1s_2 \ldots s_n \in S$ אז $yt_is \in R$ לכל $1 \leq i \leq n$ ולכן $ysI \subseteq R$ ולכן $ys \in I^{-1}$ כלומר $y \in \frac{1}{s}I^{-1} \subseteq \left(I^{-1}\right)_S$ ולכן קיבלנו $\left(I^{-1}\right)_S \supseteq (I_S)^{-1}$. ■

טענה 7.8 יהי R חוג דדקינד ו$S \subseteq R$ קבוצה כפלית. אז R_S הוא חוג דדקינד.

הוכחה: R_S תחום שלמות: כי $R_S \subseteq K$.

R_S נתר: יהי $I \subseteq R_S$ אידאל, אז ראינו כי $I = (I \cap R_S) \cdot R_S$ ומתקיים כי $I \cap R \subseteq R$ אידאל ונוצר סופית כR מודול ולכן I נוצר סופית כR_S מודול.

כל אידאל $0 \neq Q \subseteq R_S$ ראשוני הוא מקסימלי: נניח בשלילה ש

$$0 \subsetneqq Q \subsetneqq Q' \subsetneqq R_S$$

אידאלים ראשוניים. אז $Q \cap R \subseteq Q' \cap R$ אידאלים ראשוניים השונים מאפס של R (שונים מאפס כי $Q = (Q \cap R)_S, Q' = (Q' \cap R)_S$) וכמו כן $Q \cap R \subsetneqq Q' \cap R$ (אחרת $Q = Q'$ כמו קודם). סתירה לכך שכל אידאל ראשוני השונה מ0 בR הוא מקסימלי.

R_S סגור בשלמות: יהי $x \in K$ שלם מעל R_S. אז x מקיים משוואה מהצורה

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{a_0}{s_0} = 0$$

עם $a_i \in R$ ו$s_i \in S$ (לכל $0 \leq i \leq n-1$). נסמן $s = s_1 \cdot \cdots \cdot s_{n-1}$ ואז xs שלם מעל R. כי

$$(sx)^n + a_{n-1} \cdot \underbrace{\frac{s}{s_{n-1}}}_{\in R} (sx)^{n-1} + \cdots + a_0 \cdot \underbrace{\frac{s^n}{s_0}}_{\in R} = 0$$

ולכן $xs \in R$ ומכאן $x = \frac{xs}{s} \in R_S$. ■

7.2 פעולת $\alpha : I \mapsto I_S$ על הבסיס הקנוני $\{P \mid 0 \neq P \subseteq R \mid P \text{ is prime}\}$

יהי R חוג דדקינד, ותהי $S \subseteq R$ קבוצה כפלית. אז R_S חוג דדקינד ו

$$\alpha : \mathfrak{F}(R) \to \mathfrak{F}(R_S)$$

הומומורפיזם של חבורות. נסמן

$$\begin{aligned}\Sigma &= \{0 \neq P \subseteq R \mid P \text{ is prime}\}\\ \Sigma' &= \{0 \neq P \subseteq R \mid P \text{ is prime} \mid P \cap S \neq \emptyset\}\\ \Sigma'' &= \{0 \neq P \subseteq R \mid P \text{ is prime} \mid P \cap S = \emptyset\}\\ \Sigma_S &= \{0 \neq Q \subseteq R_S \mid Q \text{ is prime}\}\end{aligned}$$

1. לכל $P \in \Sigma'$ מתקיים $P_S = R_S = 1_{\mathfrak{F}(R_S)}$:
אכן, אם $s \in P \cap S$ אז $1 = \frac{s}{s} \in P_S$.

2. אם $P \in \Sigma''$ אז $P_S \cap R = P$. אכן, ברור ש$P \subseteq P_S \cap R$. בכיוון ההפוך, יהי $r \in P_S \cap R$. אז $r \in R$ ויש $p \in P$ ו$s \in S$ כך ש$r = \frac{p}{s}$ ולכן $p = rs \in P$. מכאן $s \in P$ או $r \in P$, אך מאחר ו$S \cap P = \emptyset$ מתקיים $r \in P$ ולכן $P_S \cap R \subseteq P$.

מסקנה 7.9

1. ההעתקה

$$\begin{aligned}\Sigma'' &\to \Sigma_S\\ P &\to P_S\end{aligned}$$

היא חד־חד־ערכית (כי $P_S \cap R = P$) ועל (כי $Q = (Q \cap R)_S$ לאידאל $Q \subseteq R_S$).
ההעתקה α שולחת את החלק Σ'' מהבסיס של $\mathfrak{F}(R)$ לבסיס Σ_S ושולחת את Σ' ל$1_{\mathfrak{F}(R)}$.

2. יהי $I = P_1^{n_1} \cdot \dots \cdot P_k^{n_k}$ אידאל שברי. נניח ש

$$\begin{aligned}P_1 \cap S &= \emptyset\\ &\dots\\ P_n \cap S &= \emptyset\\ P_{n+1} \cap S &\neq \emptyset\\ &\dots\\ P_k \cap S &\neq \emptyset\end{aligned}$$

ואז

$$\begin{aligned}I_S &= (P_1)_S^{n_1} \cdot \dots \cdot (P_k)_S^{n_k}\\ &= (P_{n+1})_S^{n_{n+1}} \cdot \dots \cdot (P_k)_S^{n_k}\end{aligned}$$

בפרט

$$\nu_{P_S}^{R_S}(I_S) = \nu_P^R(I)$$

7.3 מיקום באידאל ראשוני

יהי R תחום ויהי $P \subseteq R$ אידאל ראשוני. נסמן $S = R \setminus P$ ומסמנים

$$\begin{aligned} R_P &= R_S = R_{R\setminus P} \\ I_P &= I_S = I_{R\setminus P} \end{aligned}$$

בפרט $P_P = P \cdot R_S$.

טענה 7.10 ניתן לשחזר את אידאל $I \subseteq R$ בעזרת המיקומים שלו

$$I = \bigcap_{\substack{M \subseteq R \\ M \text{ is a maximal ideal}}} I_M \subseteq K$$

בפרט מתקיים

$$R = \bigcap_{\substack{M \subseteq R \\ M \text{ is a maximal ideal}}} R_M \subseteq K$$

הוכחה: $\subseteq$: ברור כי $I \subseteq I_M$ לכל אידאל $M \subseteq R$ מקסימלי.
$\supseteq$: יהי $x \in \bigcap_M I_M$, אז $x \in K$ ולכן יש $r \in R$ עם $rx \in R$. נסמן

$$J = \{r \in R \mid rx \in I\}$$

אז $J \subseteq R$ אידאל. נוכיח כי $J = R$ ואז נסיק $1 \in J$ ומכאן נקבל $y = x \cdot 1 \in I$.
אם $J \neq R$ אז קיים אידאל מקסימלי $J \subseteq M$. אבל נתון ש $x \in I_M \left(= I_{R\setminus M}\right)$ ולכן קיים $s \in R \setminus M$ כך ש$sx \in I$, כלומר $s \in J$ ו$s \notin M$. סתירה לכך ש$J \subseteq M$. ■

נניח כעת כי R חוג דדקינד ו$0 \neq P \subseteq R$ ראשוני. אז כל אידאל $0 \neq P_1 \subseteq R$ ראשוני אחר חותך את $R \setminus P$.
לכן בR_P אידאל ראשוני היחיד השונה מ0 והוא

$$P_P = P \cdot R_P = \left\{\frac{p}{s} \mid p \in P, s \notin P\right\}$$

ואם $I \subseteq K$ אידאל שברי עם פירוק

$$I = \prod_{\substack{0 \neq P' \subseteq R \\ P' \text{ is prime}}} P'^{\nu_{P'}(I)}$$

אז

$$I_P = I \cdot R_P = P_P^{\nu_P(I)}$$

כלומר

$$\nu_{P_P}(I_P) = \nu_P(I)$$

טענה 7.11 יהי R חוג נתר שאינו שדה. התנאים הבאים שקולים:

1. R חוג דדקינד
2. לכל $0 \neq P \subseteq R$ ראשוני, מתקיים כי R_P הוא DVR.
3. לכל $M \subseteq R$ מקסימלי, מתקיים כי R_M הוא DVR.

הוכחה: $2 \implies 1$: ראינו, כי הוכחנו כי כל חוג דדקינד עם אידאל ראשוני השונה מאפס יחיד הוא DVR.
$3 \implies 2$: ברור.
$1 \implies 3$: נראה שכל אידאל שברי $I \subseteq K$ הוא הפיך. ע"י כפל באיבר מ$K^{\times}$ אפשר להניח כי I שלם. עלינו להראות כי $II^{-1} = R$.
יהי M אידאל מקסימלי, מאחר וR נתר, מתקיים כי I נוצר סופית וראינו שנובע

$$\left(I^{-1}\right)_M = \left(I_M\right)^{-1}$$

לכן

$$\left(II^{-1}\right)_M = I_M\left(I_M^{-1}\right) = I_M\left(I_M\right)^{-1} = R_M$$

כאשר השוויון האחרון נכון כי R_M הוא חוג DVR ולכן דדקינד. לבסוף מתקיים

$$II^{-1} = \bigcap_M \left(II^{-1}\right)_M = \bigcap_M R_M = R$$

■

8 הרחבות סופיות ספרביליות של חוג דדקינד

(תזכורת): תהי K/F הרחבה ספרבילית סופית של שדות, אזי יש העתקה F-לינארית

$$\mathrm{Tr} = \mathrm{Tr}_{K/F} : K \to F$$

עם התכונות הבאות:

1. $\mathrm{tr} \neq 0$ ולכן התבנית

$$\begin{aligned} K \times K &\to F \\ (x,y) &\mapsto \mathrm{Tr}\left(x \cdot y\right) \end{aligned}$$

לא מנוונת. (כי אם $\mathrm{Tr}\left(x_0\right) \neq 0$, אז לכל $x \in K^{\times}$ ניקח $y = \frac{x_0}{x}$ ואז $\mathrm{Tr}\left(xy\right) \neq 0$) לכן לכל בסיס $u_1, \ldots, u_n$ (כאשר $n = [K : F]$) יש בסיס דואלי $v_1, \ldots, v_n$ במובן ש $\mathrm{Tr}\left(u_i v_j\right) = \delta_{ij} \in F$.

2. יהי $\mathcal{O}$ תחום, F שדה המנות של $\mathcal{O}$ ונניח כי $\mathcal{O}$ סגור בשלמות. תהי K/F הרחבה ספרבילית סופית. לכל $\alpha \in K$, יהיו

$$F\left[x\right] \ni \quad m\left(x\right) = x^l + c_{l-1}x^{l-1} + \cdots + c_0$$

הפולינום המינימלי של α מעל F ו

$$F\left[X\right]\ni f\left(x\right) = \det\left(x\mathrm{Id}-\alpha\right)=x^{n}+b_{n-1}x^{n-1}+\cdots+b_{0}$$

הפולינום האופייני של α. כאשר

$$\begin{aligned}\alpha:K & \to K\\ v & \mapsto \alpha\cdot v\end{aligned}$$

(כאשר $n=\left[K:F\right]$, $l=\left[F\left(\alpha\right):F\right]$)

הערה 8.1 f היא חזקה של m.

טענה 8.2 התנאים הבאים שקולים:

1. α שלם מעל $\mathcal{O}$
2. המקדמים c_i של m הם ב$\mathcal{O}$
3. המקדמים b_j של f הם ב$\mathcal{O}$

הוכחה: $2 \Longleftarrow 3$ לפי ההערה.
$3 \Longleftarrow 1$: מיידי (כי $\mathcal{O}\subseteq F$)
$1 \Longleftarrow 2$: יהי F^{al} הסגור האלגברי של F. כל שורשי m שלמים מעל $\mathcal{O}$ ולכן כל מקדמי m שלמים מעל $\mathcal{O}$ ולכן ב$\mathcal{O}$. (כי הם בF, וכי $\mathcal{O}$ סגור בשלמות) ■

מסקנה 8.3 בפרט נובע כי $\mathrm{Tr}_{K/F}\left(\alpha\right),N_{K/F}\left(\alpha\right)\in\mathcal{O}$.

יהיו $\mathcal{O}\subseteq R$ תחומים ונניח שR שלם מעל $\mathcal{O}$. ברור שאם $Q\subseteq R$ אידאל ראשוני, אז $P=Q\cap\mathcal{O}$ אידאל ראשוני ב$\mathcal{O}$. אומרים "Q מעל P" או "P מתחת לQ".

טענה 8.4 $\mathcal{O}$ שדה $\Longleftrightarrow$ R שדה.

הוכחה: $\Longrightarrow$: נניח שR שדה. יהי $0\neq x\in\mathcal{O}$, אז קיים $\frac{1}{x}\in R$ והינו שלם מעל $\mathcal{O}$ ולכן מתקיימת משוואה מהצורה

$$\frac{1}{x^{n}}+\frac{a_{n-1}}{x^{n-1}}+\cdots+\frac{a_{1}}{x}+a_{0} = 0$$

כאשר $a_i\in\mathcal{O}$ ו$n\geq1$. מכאן

$$1+x\left(a_{n-1}+\cdots+a_{1}x^{n-2}+a_{0}x^{n-1}\right) = 0$$

ומכאן שx הפיך ב$\mathcal{O}$.
$\Longleftarrow$: נניח ש$\mathcal{O}$ שדה. יהי $0\neq y\in R$. אז y מקיים משוואה מהצורה

$$y^{k}+b_{k-1}y^{k-1}+\cdots+b_{0} = 0$$

(כאשר $k\geq1$)
אפשר להניח $b_0\neq0$ ואז b_0 הפיך בחוג $\mathcal{O}$ ומתחלק בy (בחוג R) ולכן y הפיך בR. ■

מסקנה 8.5 יהי $R \subseteq Q$ אידאל ראשוני. נסמן $P = Q \cap \mathcal{O}$. אז Q מקסימלי בR $\iff$ P מקסימלי ב$\mathcal{O}$.

הוכחה: מאחר וR שלם מעל $\mathcal{O}$, מתקיים כי R/Q שלם מעל $\mathcal{O}/P$ ולכן R/Q שדה $\iff$ $\mathcal{O}/P$ שדה. ■

טענה 8.6 יהי $\mathcal{O} \subseteq P$ אידאל ראשוני. אז קיים אידאל ראשוני $R \subseteq Q$ כך ש$Q \cap \mathcal{O} = P$. בפרט $PR \neq R$.

הוכחה: R_P תחום ו$\mathcal{O}_P \subseteq R_P$ וR_P שלם מעל $\mathcal{O}_P$. אכן, אם $\frac{x}{s} \in R_P$ כאשר $x \in R$ ו$s \in R \setminus P$ אז x מקים משוואה מהצורה

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 \quad = \quad 0$$

כאשר לכל i מתקיים $c_i \in \mathcal{O}$. לכן מתקיים

$$\left(\frac{x}{s}\right)^n + \frac{c_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{c_0}{s^n} \quad = \quad 0$$

ולכן $\frac{x}{s}$ שלם ביחס ל$\mathcal{O}_S$ כאשר $S = R \setminus P$.

כעת, יהי M אידאל מקסימלי כלשהו של R_P אז $\mathcal{O}_P \cap M$ מקסימלי ב$\mathcal{O}_P$ (מהמסקנה) ולכן $\mathcal{O}_P \cap M = P_P$.

נסתכל על התרשים

$$\begin{array}{ccc} R & \subseteq & R_P \\ \cup & & \cup \\ \mathcal{O} & \subseteq & \mathcal{O}_P \end{array}$$

נסמן $Q = R \cap M$, אז Q ראשוני בR ומתקיים

$$\mathcal{O} \cap Q \quad = \quad \mathcal{O} \cap M = \mathcal{O} \cap (\mathcal{O}_P \cap M) = \mathcal{O} \cap P_P = P$$

■

הערה 8.7 יהי $\mathcal{O}$ חוג דדקינד עם שדה מנות F. תהי K/F הרחבת שדות. R הסגור השלם של $\mathcal{O}$ בF. אז ידוע שR חוג. לכל איבר $x \in K$ יש תיאור $x = \frac{r}{a}$ כאשר $r \in R$ ו$a \in \mathcal{O} \setminus \{0\}$. בפרט, שדה המנות של R הוא K.

הוכחה: x מקיים משוואה מהצורה

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 \quad = \quad 0$$

עם $c_i \in F$ לכל $0 \leq i \leq n-1$. קיים $a \in \mathcal{O} \setminus \{0\}$ כך ש$ac_i \in \mathcal{O}$ (לכל i). נסמן $r = ax$, אז

$$r^n + ac_{n-1}r^{n-1} + \cdots + a^n c_0 \quad = \quad 0$$

ולכן $r \in R$ ולכן $x = \frac{ax}{a} = \frac{r}{a}$ כנדרש. ■

8.1 הרחבות ספרביליות של חוגי דדקינד

משפט 8.8 יהי $\mathcal{O}$ חוג דדקינד עם שדה מנות F. תהי K/F הרחבה ספרבילית סופית של שדות, ויהי $K \subseteq R$ הסגור השלם של $\mathcal{O}$ בK. אז R חוג דדקינד וR מודול נוצר סופית מעל $\mathcal{O}$.

הוכחה: יהי $u_1, \ldots, u_n$ בסיס של K/F ($n = [K:F]$). ראינו ש(ע"י כפל באיברים מ$F^\times$), אפשר להניח כי $u_1, \ldots, u_n \in R$. יהי $v_1, \ldots, v_n$ הבסיס הדואלי. נראה ש $R \subseteq \sum_{i=1}^n \mathcal{O} v_i$. אכן, יהי $x \in R$, אז יש $\gamma_i \in F$ ($i = 1, \ldots, n$) עם $x = \sum_{i=1}^n \gamma_i v_i$ ואז

$$\forall j \quad \mathrm{Tr}\left(x u_j\right) \quad = \sum_{i=1}^n \gamma_i \mathrm{Tr}\left(v_i u_j\right) = \gamma_j$$

אבל $x u_j \in R$ ולכן $\gamma_j = \mathrm{Tr}\left(x u_j\right) \in \mathcal{O}$. מכאן נובע ש$R$ מוכל ב$\mathcal{O}$-מודול נוצר סופית, אבל $\mathcal{O}$ נתר ולכן R נוצר סופית כ$\mathcal{O}$-מודול.

נראה כי R חוג דדקינד:

- R תחום - מיידי
- R נתר - כי כל אידאל $I \subseteq R$ נוצר סופית אפילו כ$\mathcal{O}$-מודול.
- R סגור בשלמות: כי R הוא הסגור השלם של $\mathcal{O}$ בK.

נותר להוכיח כי אם $0 \neq Q \subseteq R$ אידאל ראשוני אז Q מקסימלי. לצורך זה, מספיק להראות ש$P = Q \cap \mathcal{O}$ שונה מאפס. (אכן, מכאן ינבע כי P מקסימלי ב$\mathcal{O}$ ולכן Q מקסימלי בR)

יהי $0 \neq x \in Q$. אז x שלם מעל $\mathcal{O}$ ולכן מקיים משוואה מהצורה

$$x^k + a_{k-1} x^{k-1} + \cdots + a_0 \quad = \quad 0$$

(כאשר $k \geq 1$ ו$a_i \in \mathcal{O}$ לכל i)

מאחר וR תחום, אפשר להניח כי $a_0 \neq 0$ ואז

$$-a_0 \quad = \quad x^k + a_{k-1} x^{k-1} + \cdots + a_1 x \subseteq \mathcal{O} Q \subseteq R Q = Q$$

לכן $0 \neq a_0 \in Q \cap \mathcal{O} = P$. לכן $P \neq 0$ כנדרש. ■

מסקנה 8.9 באותם סימונים, אם $\mathcal{O}$ הוא גם חוג ראשי אז:

1. R מודול חופשי מעל $\mathcal{O}$.
2. כל בסיס של R מעל $\mathcal{O}$ הוא גם בסיס של K מעל F.

הוכחה:

1. R נוצר סופית ללא פיתול מעל חוג ראשי.
2. נובע מכך שלכל $x \in K$ יש תיאור $x = \frac{r}{a}$ כאשר $r \in R$ ו$a \in \mathcal{O} \setminus \{0\}$.

■

נשתמש במסקנה זו כאשר $\mathcal{O} = \mathbb{Z}$ או כאשר $\mathcal{O}$ הוא DVR.

הגדרה 8.10 שדה מספרים K הוא הרחבה סופית של $\mathbb{Q}$. במצב זה, הסגור השלם $\mathcal{O}_K$ של $\mathbb{Z}$ בK הוא חוג דדקינד. $\mathcal{O}_K$ הוא מודול חופשי מעל $\mathbb{Z}$.

8.2 f

יהי $\mathcal{O}$ חוג דדקינד עם שדה מנות F, K/F הרחבה ספרבילית סופית $R\subseteq K$ הסגור השלם מעל $\mathcal{O}$. יהי $0\neq Q\subseteq R$ ראשוני. אז $P=Q\cap R$ מקיים ש$P\neq 0$ (כי Q מקסימלי ולכן P מקסימלי)

ברור שיש שיכון של שדות $\mathcal{O}/P\hookrightarrow R/Q$ ומסמנים $f_Q=[R/Q:\mathcal{O}/P]$.

הערה 8.11 f נשמר ע"י מיקום $f_Q=\left[\frac{R_P}{Q_P}:\frac{\mathcal{O}_P}{P_P}\right]$ ואכן $\frac{\mathcal{O}_P}{P_P}=\frac{\mathcal{O}}{P}$ ו$\frac{R}{Q}=\frac{R_P}{Q_P}$.

הוכחה: כל $s\in S=\mathcal{O}\setminus P$ הפיך ב$\mathcal{O}/P$ (כי P מקסימלי ולכן $R=P+sR$. ולכן קיימים $a,b\in\mathcal{O}$ ו$p\in R$ עם $as+bp=1$ ואז ב$\mathcal{O}/P$ מתקיים $(s+P)(a+P)=1+P$ ו$s+P$ הפיך)

לכן $R/Q=(R/Q)_P=R_P/Q_Q$ נסתכל על הסדרה המדויקת

$$0\to Q\to R\quad\to\quad R/Q\to 0$$

ולוקאליזציה היא פעולה מדויקת ובנוסף

$$\mathcal{O}/P\quad=\quad(\mathcal{O}/P)_P=\frac{\mathcal{O}_P}{P_P}$$

■

8.3 הרחבת אידאלים (הומומורפיזם הinjection)

יהי $\mathcal{O}$ חוג דדקינד עם שדה מנות F. K/F הרחבה ספרבילית סופית של שדות, ו$R\subseteq K$ הסגור השלם של $\mathcal{O}$ בK. יש הומומורפיזם של חבורות

$$\begin{aligned} i:\mathfrak{F}(\mathcal{O}) &\to \mathfrak{F}(R)\\ J &\mapsto JR\end{aligned}$$

i מוגדר כי J נוצר סופית מעל $\mathcal{O}$ ושונה מאפס $\Longleftarrow$ JR נוצר סופית מעל R ושונה מאפס. מתקיים

$$(J_1R)(J_2R)\quad=\quad(J_1J_2)R$$

למשל נובע

$$J^{-1}R\quad=\quad(JR)^{-1}$$

יהי $P\subseteq\mathcal{O}$ אידאל ראשוני, אז $0\neq PR\subseteq R$ אידאל בR ומתקיים $PR\neq R$ (ראינו). ממשפט הפירוק

$$PR\quad=\quad Q_1^{e_1}\cdot\dots\cdot Q_r^{e_r}$$

עם $e_i\geq 1$ ו$Q_1,\dots,Q_r\subseteq R$ ראשוניים השונים מאפס ושונים זה מזה.

עבור $0\neq Q\subseteq R$ התנאים הבאים שקולים: קיים $Q=Q_i\iff PR\subseteq Q$ (תכונות פירוק) $\iff P\subseteq Q$ (ראינו $PR\cap\mathcal{O}=P$) $\iff P\subseteq\mathcal{O}\cap Q\iff P=\mathcal{O}\cap Q$.
מכאן $Q_1,\dots,Q_r$ הם בדיוק האידאלים הראשוניים של R מעל P. בפרט i היא העתקה חד־חד־ערכית.

מסקנה 8.12 לכל $0 \neq P \subseteq \mathcal{O}$ ראשוני יש רק מספר סופי של אידאלים ראשוניים $0 \neq Q_1, \dots, Q_r \subseteq R$ מעל P.

הערה 8.13 R_P הוא הסגור השלם של $\mathcal{O}_P$ ומ

$$PR = Q_1^{e_1} \cdot \dots \cdot Q_r^{e_r}$$

נובע

$$PR_P = (Q_1)_P^{e_1} \cdot \dots \cdot (Q_r)_P^{e_r}$$

8.4 e

יהי $0 \neq Q \subseteq R$ אידאל ראשוני. נסמן $P = Q \cap \mathcal{O}$ אידאל מקסימלי ב$\mathcal{O}$ (כי Q מקסימלי בR). ולכן $P \neq 0$ ראשוני. אז Q מופיע בפירוק

$$PR = Q_1^{e_1} \cdot \dots \cdot Q_r^{e_r}$$

יהי i כך ש$Q = Q_i$ ונסמן $e_Q = e_i$.

הערה 8.14 $e_Q \geq 1$ ו$e_{QR_P} = e_Q$.

הגדרה 8.15 אם $e_Q = 1$ והרחבת השדות $(R/Q) / (\mathcal{O}/P)$ ספרבילית, אומרים שQ לא מסועף

הגדרה 8.16 אם $0 \neq P \subseteq \mathcal{O}$ ראשוני ו$PR = Q_1^{e_1} \cdot \dots \cdot Q_r^{e_r}$ הפירוק, אומרים שP לא מסועף אם כל Q_i לא מסועף.

8.5 $\sum_{i=1}^n e_i f_i = [K : F]$

טענה 8.17 יהי $\mathcal{O}$ חוג דדקינד עם שדה מנות F. תהי K/F הרחבה ספרבילית סופית. יהי $R \subseteq K$ הסגור השלם של $\mathcal{O}$.
יהי $0 \neq P \subseteq \mathcal{O}$ אידאל ראשוני. אז R/RP מרחב וקטורי מעל $\mathcal{O}/P$ (מיידי) ומתקיים $\dim_{\mathcal{O}/P}(R/RP) = [K : F]$.

הוכחה: נעבור למיקום בP: R_P הוא הסגור השלם של $\mathcal{O}_P$. בנוסף $\mathcal{O}_P$ הוא DVR ולכן חוג ראשי ולכן $R_P \cong \mathcal{O}_P^n$ כאשר $n = [K : F]$ (זה נובע מכך שהסברנו שכל בסיס של R_P מעל O_P הוא גם בסיס של K מעל F). לכן

$$R_P/PR_P \cong (\mathcal{O}_P/P\mathcal{O}_P)^n$$

ולבסוף

$$\dim_{\mathcal{O}/P}(R/RP) = \dim_{\mathcal{O}_P/P_P}(R_P/PR_P) = n = [K : F]$$

■

למה 8.18 יהי R חוג דדקינד $0 \neq Q \subseteq R$ ראשוני. אז לכל $n \geq 1$ יש איזומורפיזם של R/Q-מרחבים וקטוריים:

$$R/Q \quad \cong \quad Q^n/Q^{n+1}$$

טענה 8.19 בסימונים אלה יהי $0 \neq P \subseteq \mathcal{O}$ ראשוני ו$PR = Q_1^{e_1} \cdot \dots \cdot Q_r^{e_r}$ הפירוק. אז

$$\sum_{i=1}^{r} e_i f_i \quad = \quad [K:F]$$

הוכחה: ראינו ש

$$\dim_{\mathcal{O}/P}(R/PR) \quad = \quad n = [K:F]$$

לפי משפט השאריות הסיני והפירוק PR מתקיים

$$P/PR \quad = \quad \bigoplus_{i=1}^{n} R/Q^{e_i}$$

כסכום ישר של $\mathcal{O}/P$-מרחבים וקטוריים. לכן די להראות ש

$$\dim_{\mathcal{O}/P}(R/Q_i^{e_i}) \quad = \quad e_i f_i$$

יש פילטרציה

$$0 = Q_i^{e_i}/Q_i^{e_i} \quad \subseteq \dots \quad \subseteq Q_i^2/Q_i^{e_i} \subseteq Q_i^1/Q_i^{e_i} \subseteq Q_i^0/Q_i^{e_i} = R/Q_i^{e_i}$$

של $\mathcal{O}/P$-מרחבים וקטוריים. לכן די להראות כי

$$\dim_{\mathcal{O}/P}\left(\left(Q_i^j/Q_i^{e_i}\right)/\left(Q_i^{j+1}/Q_i^{e_i}\right)\right) \quad = \quad f_i$$

כלומר ש

$$\dim_{\mathcal{O}/P}\left(Q_i^j/Q_i^{j+1}\right) \quad = \quad f_i$$

אבל זה נכון לאור האיזומופיזם של $\mathcal{O}/P$-מרחבים וקטוריים

$$R/Q_i \quad \cong \quad Q_i^j/Q_i^{j+1}$$

ומכך שf_i מוגדר כמימד

$$f_i \quad = \quad \dim_{\mathcal{O}/P}(R/Q_i)$$

■

מסקנה 8.20

1. $1 \leq f_Q < \infty$
2. בפרט אם K שדה מספרים, $R \subseteq K$ המספרים השלמים נקח $F = \mathbb{Q}$, $\mathcal{O} = \mathbb{Z}$, אז לכל $p \in \mathbb{Z}$ מתקיים כי $\mathbb{Z}/p\mathbb{Z}$ שדה ולכן לכל $Q \subseteq R$ ראשוני השונה מ0 מתקיים כי R/Q שדה סופי. (הרחבה מימד f_Q של $\mathbb{Z}/p\mathbb{Z}$)

8.6 משפט קומר־דדקינד על הפירוק

יהי $\mathcal{O}$ חוג דדקינד, F שדה המנות, K/F ספרבילית סופית, $R \subseteq K$ הסגור השלם של $\mathcal{O}$.
יהי $0 \neq P \subseteq \mathcal{O}$ ראשוני עם ההנחה הבאה:
הנחה: נניח כי קיים $\alpha \in K$ כך ש$R_P = \mathcal{O}_P[\alpha]$.

הערה 8.21 כאן ובהמשך:

$$\begin{aligned} R_P &= \left\{ \frac{r}{s} \mid r \in P, s \in \mathcal{O} \setminus P \right\} \\ \mathcal{O}[\alpha]_P &= \left\{ \frac{t}{s} \mid t \in \mathcal{O}[\alpha], s \in \mathcal{O} \setminus P \right\} \\ \mathcal{O}_P &= \left\{ \frac{x}{s} \mid x \in \mathcal{O}, s \in \mathcal{O} \setminus P \right\} \end{aligned}$$

הערה 8.22 $\mathcal{O}_P[\alpha] = \mathcal{O}[\alpha]_P$

מסקנה 8.23 מההנחה $R_P = \mathcal{O}_P[\alpha]$ מתקיים כי:

1. $F[\alpha] = K$
2. לכל $r \in R$ קיים $s \in \mathcal{O} \setminus P$ כך ש$r \cdot s \in \mathcal{O}[\alpha]$, כי

$$r = \frac{r}{1} \in R_P = \mathcal{O}[\alpha]_P$$

ולכן $r = \frac{t}{s}$ כאשר $t \in \mathcal{O}[\alpha]$ ו$s \in \mathcal{O} \setminus P$ מתאימים.

למה 8.24 ההכלה $R \hookrightarrow \mathcal{O}[\alpha]$ משרה איזומורפיזם

$$\varphi : \mathcal{O}[\alpha] / P\mathcal{O}[\alpha] \cong R/PR$$

מעל $\mathcal{O}/P$.

הוכחה: ברור שφ מוגדר היטב. נוכיח שφ על. יהי $r \in R$, יהיו $t \in \mathcal{O}[\alpha]$ ו$s \in \mathcal{O} \setminus P$ כך ש $rs = t$. מאחר ו$s\mathcal{O} + P = \mathcal{O}$ (כי P אידאל ראשוני ולכן מקסימלי), קיימים $a \in \mathcal{O}$ ו$p \in P$ כך ש$sa + p = 1 \in \mathcal{O}$. ברור ש$ta \in \mathcal{O}[\alpha]$ ו$r + PR \in R/PR$ ומתקיים

$$\begin{aligned} r + PR &= rsa + pr + PR \\ &= rsa + PR \\ &= ta + PR \\ &= \varphi(ta + P\mathcal{O}[\alpha]) \end{aligned}$$

ולכן φ על.
נראה כי φ חד־חד־ערכית: יהי $t \in \mathcal{O}[\alpha]$ כך ש

$$\begin{aligned} \varphi(t + P\mathcal{O}[\alpha]) &= 0 \\ t + PR &= 0 \end{aligned}$$

לכן $t \in PR$, כלומר יש שוויון $t = \sum_j p_j r_j$ ($p_j \in P$, $r_j \in R$). לכן קיים $s \in \mathcal{O} \setminus P$ כך ש$ts \in P\mathcal{O}[\alpha]$. שוב יש $p \in P$ ו$a \in \mathcal{O}$ כך ש$as + p = 1 \in \mathcal{O}$ ואז $pt \in P\mathcal{O}[\alpha]$ (כי כזכור $t \in \mathcal{O}[\alpha]$) ואז

$$t = (as+p)\,t \in aP\mathcal{O}[\alpha] + P\mathcal{O}[\alpha] = P\mathcal{O}[\alpha]$$

ולכן t מייצג את 0 ב$\mathcal{O}[\alpha]/P\mathcal{O}[\alpha]$. כנדרש. ■

נציג הוכחה נוספת: **הוכחה:** יש סדרה מדויקת של $\mathcal{O}$ מודולים

$$0 \to \mathcal{O}[\alpha] \to R \to M \to 0$$

ונתון ש$M_P = 0$. מהסדרה מתקבלת סדרה מדויקת

$$\mathrm{Tor}_1^{\mathcal{O}}(\mathcal{O}/P, M) \to \mathcal{O}/P \otimes_{\mathcal{O}} \mathcal{O}[\alpha] \to \mathcal{O}/P \otimes_{\mathcal{O}} R \to \mathcal{O}/P \otimes_{\mathcal{O}} M = \mathrm{Tor}_0^{\mathcal{O}}(\mathcal{O}/P, M)$$

לכל אידאל מקסימלי $P' \neq P$ מתקיים $(\mathcal{O}/P)_{P'} = 0$ וכמו כן $M_P = 0$ ולכל חוג חילופי R ו $S \subseteq R$ קבוצה כפלית, A, B R־מודולים מתקיים

$$S^{-1}\mathrm{Tor}_n^R(A,B) = \mathrm{Tor}_n^{S^{-1}R}\left(S^{-1}A, S^{-1}B\right)$$

(פרטים נוספים ניתן למצוא ב- An Introduction to Homological Algebra (Universitext), עמוד 415, טענה 7.17) ■

יהי $f = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ הפולינום המינימלי של α מעל F. אז $n = [K:F]$. מאחר שα שלם מעל $\mathcal{O}$, מתקיים $c_i \in \mathcal{O}$. נסמן את העתקת המנה

$$\begin{aligned} \bar{\cdot} : \mathcal{O} &\to \mathcal{O}/P \\ a &\mapsto \overline{a} = a + P \end{aligned}$$

נרחיב אותה ל

$$\begin{aligned} \bar{\cdot} : \mathcal{O}[x] &\to \overline{\mathcal{O}}[x] \\ \overline{\sum_i b_i x^i} &= \sum_i \overline{b_i} x^i \end{aligned}$$

כאשר $\overline{\mathcal{O}} = \mathcal{O}/P$. מאחר שמקדמי f ב$\mathcal{O}$ מתקיים כי $\mathcal{O}[\alpha] = \mathcal{O} \oplus \alpha\mathcal{O} \oplus \cdots \oplus \alpha^{n-1}\mathcal{O}$ הוא סכום ישר של $\mathcal{O}$ מודולים.

יש הומומורפיזם של $\overline{\mathcal{O}}$ אלגבראות:

$$\overline{\mathcal{O}} = \mathcal{O}/P \to \mathcal{O}[\alpha]/P\mathcal{O}[\alpha]$$

המתקבל מ$\mathcal{O} \hookrightarrow \mathcal{O}[\alpha]$ מכאן מקבלים הומומורפיזם של $\overline{\mathcal{O}}$ אלגבראות

$$\overline{\mathcal{O}}[x] \to \mathcal{O}[\alpha]/P\mathcal{O}[\alpha]$$

השולח את x ל$\alpha + P\mathcal{O}[\alpha]$. מאחר ש$f(\alpha) = 0$ נובע ש$\overline{f}(x) \in \mathcal{O}[\alpha]$ נשלח ל$0 \ni \mathcal{O}[\alpha]/P\mathcal{O}[\alpha]$ ולכן נקבל הומומורפיזם של $\overline{\mathcal{O}}$ אלגבראות

$$\varphi_1 : \overline{\mathcal{O}}[x]/\left(\overline{f}\right) \to \mathcal{O}[\alpha]/P\mathcal{O}[\alpha]$$

למה 8.25 φ_1 איזומורפיזם של $\overline{\mathcal{O}}$ אלגבראות.

הוכחה:

$$\mathcal{O}[\alpha]/P\mathcal{O}[\alpha] = \overline{\mathcal{O}} \oplus \overline{\alpha}\overline{\mathcal{O}} \oplus \cdots \oplus \overline{\alpha}^{n-1}\mathcal{O}$$

כמו כן

$$\overline{\mathcal{O}}[x]/\left(\overline{f}\right) = \overline{\mathcal{O}} \oplus x\overline{\mathcal{O}} \oplus \cdots \oplus x^{n-1}\mathcal{O}$$

(למעשה צריך לכתוב $\overline{\mathcal{O}}\left(x+\left(\overline{f}\right)\right)$ ו$\overline{\mathcal{O}}\left(x^{n-1}+\left(\overline{f}\right)\right)$ אבל זה מאריך את הכתיבה)
זה נכון כי f מתוקן. φ_1 היא הזהות על $\overline{\mathcal{O}}$ ברכיב הראשון וφ_1 שולח את הקוסט של x לקוסט של α. מכאן חד־חד־ערכיות ועל ברורה. ■

משפט 8.26 בסימונים לעיל יהי

$$\overline{f}(x) = G_1(x)^{e_1} \cdot \cdots \cdot G_n(x)^{e_n}$$

הפירוק של $\overline{f} \in \overline{\mathcal{O}}[x]$ לפולינומים אי־פריקים מתוקנים, כאשר $G_1, \ldots, G_n$ שונים זה מזה ו$e_i \geq 1$ (לכל i). יהיו $g_i(x) \in \mathcal{O}[x]$ פולינומים מתוקנים כך ש$\overline{g_i} = G_i$ (לכל i). נסמן אידאלים בR ע"י

$$Q_i = g_i(\alpha)R + PR$$

אז $Q_1, \ldots, Q_n$ אידאלים ראשוניים השונים מאפס ושונים זה מזה ומתקיים הפירוק

$$PR = Q_1^{e_1} \cdot \cdots \cdot Q_n^{e_n}$$

לבסוף לכל i מתקיים

$$\left([R/Q_i : \mathcal{O}/P] =\right) f_{Q_i} = \deg G_i = \deg g_i$$

הוכחה: נשתמש באיזומורפיזם של $\overline{\mathcal{O}}$ אלגבראות:

$$\overline{\mathcal{O}}[x]/\left(\overline{f}\right) \overset{\varphi_1}{\underset{\cong}{\rightarrow}} \mathcal{O}[\alpha]/P\mathcal{O}[\alpha] \overset{\varphi}{\underset{\cong}{\rightarrow}} R/PR$$

מאחר שG_i אי־פריק, $G_i\overline{\mathcal{O}}[x] \subseteq \overline{\mathcal{O}}[x]$ אידאל ראשוני השונה מאפס, המכיל את $\left(\overline{f}\right) = \overline{f}\mathcal{O}[x]$. מכאן נובע כי

$$G_i\overline{\mathcal{O}}[x] + \left(\overline{f}\right) \subseteq \overline{\mathcal{O}}[x]/\left(\overline{f}\right)$$

אידאל ראשוני (לכל i). בנוסף האידאלים

$$G_i\overline{\mathcal{O}}[x] + \left(\overline{f}\right) \subseteq \overline{\mathcal{O}}[x]/\left(\overline{f}\right)$$

שונים זה מזה (ל$i = 1, \ldots, n$) ־ זאת מאחר ואלה תמונות מנה של אידאלים השונים זה מזה המכילים את הגרעין $\left(\overline{f}\right)$.

נשים לב כי ממשפט האיזומורפזים השלישי מתקיים

$$\left[\frac{\overline{\mathcal{O}}\left[x\right]/\left(\overline{f}\right)}{G_{i}\overline{\mathcal{O}}\left[x\right]+\left(\overline{f}\right)}:\overline{\mathcal{O}}\right] = \left[\frac{\overline{\mathcal{O}}\left[x\right]}{G_{i}\overline{\mathcal{O}}\left[x\right]}:\overline{\mathcal{O}}\right]=\deg G_{i}$$

לבסוף מתקיים ב$\overline{\mathcal{O}}\left[x\right]/\left(\overline{f}\right)$:

$$\prod_{i}\left(G_{i}\overline{\mathcal{O}}\left[x\right]+\left(\overline{f}\right)\right)^{e_{i}} = \left(\overline{f}\right)=0_{\overline{\mathcal{O}}\left[x\right]/\left(\overline{f}\right)}$$

יהי $\widetilde{Q_{i}}\subseteq R/PR$ התמונה של האידאל $G_{i}\overline{\mathcal{O}}\left[x\right]+\left(\overline{f}\right)\subseteq\overline{\mathcal{O}}\left[x\right]/\left(\overline{f}\right)$ ביחס לאיזומורפיזם $\varphi\circ\varphi_{1}$ לעיל. אז:

1. $\widetilde{Q_{i}}$ ראשוני
2. $\left[\frac{R/PR}{\widetilde{Q_{i}}}:\overline{\mathcal{O}}\right]=\deg G_{i}$
3. $\widetilde{Q_{1}},\ldots,\widetilde{Q_{n}}$ שונים זה מזה.
4. $\prod_{i=1}^{n}\widetilde{Q_{i}}=0_{R/PR}$

לבסוף נסתכל על העתקת המנה $h:R\to R/PR$ ותהיינה $Q_{i}\subseteq R$ התמונות ההופכות $Q_{i}=h^{-1}\left(\widetilde{Q_{i}}\right)$ (לכל i). אז Q_{i} נתון ע"י הנוסחה מהמשפט $Q_{i}=g_{i}\left(\alpha\right)R+PR$.
כמו כן $Q_{i}\subseteq R$ ראשוני השונה מאפס ו$Q_{1},\ldots,Q_{n}$ שונים זה מזה ו$Q_{i}\cap\mathcal{O}=P$ (כי $1\notin Q_{i}$ ו$Q_{i}\cap\mathcal{O}\supseteq P$). וכמו כן

$$f_{Q_{i}} = \left[R/Q_{i}:\mathcal{O}/P\right]=\deg G_{i}$$

לבסוף מ4 נובע כי

$$\prod_{i=1}^{n}Q_{i}^{e_{i}} \subseteq PR$$

לכן יש מספרים $0\leq\varepsilon_{i}\leq e_{i}$ כך ש

$$PR = \prod_{i=1}^{n}Q_{i}^{\varepsilon_{i}}$$

ומכאן

$$\prod_{i=1}^{n}\widetilde{Q_{i}}^{\varepsilon_{i}} = 0_{P/PR}$$

ומשוויון זה מסיקים כי לא ייתכן $\varepsilon_{i}<e_{i}$. ■

8.7 דוגמה: הרחבות ריבועיות של $\mathbb{Q}$

יהי $d\neq 0$ שלם ללא מחלקים ריבועיים. נסמן $K=\mathbb{Q}\left(\sqrt{d}\right)$ ויהי R הסגור השלם של $\mathbb{Z}$ בK. יהי $\gamma=t+s\sqrt{d}\in K$ (באשר $t,s\in\mathbb{Q}$) הפולינום המינימלי הוא $x^2-\mathrm{Tr}_{K/\mathbb{Q}}(\gamma)+N_{K/\mathbb{Q}}(\gamma)$. מתקיים $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma)=2t$, $N_{K/\mathbb{Q}}(\gamma)=t^2-d\cdot s^2$ ולכן $2t\in\mathbb{Z}$ ו $t^2-d\cdot s^2\in\mathbb{Z}$. מכאן $d(2s)^2=4ds^2=\mathrm{Tr}_{K/\mathbb{Q}}(\gamma)^2-4N_{K/\mathbb{Q}}(\gamma)\in\mathbb{Z}$.

מאחר וd לא מתחלק בריבוע, נובע כי $2s\in\mathbb{Z}$. לכן קיימים $a,b\in\mathbb{Z}$ כך ש $\gamma=\dfrac{a+b\sqrt{d}}{2}$.

נניח $\gamma=\dfrac{a+b\sqrt{d}}{2}$ כאשר $a,b\in\mathbb{Z}$. נבדוק מתי γ שלם אלגברי מעל $\mathbb{Z}$. נדרוש $\mathrm{Tr}_{K/\mathbb{Q}}(\gamma)=a\in\mathbb{Z}$, $N_{K/\mathbb{Q}}(\gamma)=\dfrac{a^2-db^2}{4}\in\mathbb{Z}$ כלומר $4\mid a^2-db^2$.

במקרה הראשון $d\equiv 1\pmod 4$. במקרה זה $4\mid a^2-db^2$ קורה כאשר a,b שניהם זוגיים או אי־זוגיים ביחד. לכן בסיס של R במקרה זה נתון ע"י $\left\{1,\dfrac{1+\sqrt{d}}{2}\right\}$.

במקרה שני $d\equiv 2,3\pmod 4$. נשים לב כי לכל n שלם מתקיים $n^2\in\{0,1\}\pmod 4$ ולכן נקבל תנאי

$$4\quad\mid\quad\begin{pmatrix}0\\ \text{or}\\ 1\end{pmatrix}-\begin{pmatrix}2\\ \text{or}\\ 3\end{pmatrix}\cdot\begin{pmatrix}0\\ \text{or}\\ 1\end{pmatrix}$$

מכאן מקבל כי $a^2,b^2\equiv 0\pmod 4$ ולכן a,b שניהם זוגיים, ולכן בסיס לR מעל $\mathbb{Z}$ נתון ע"י $\left\{1,\sqrt{d}\right\}$.

יישום משפט קומר נבחר $\alpha=\sqrt{d}$ ויהי p ראשוני.

במקרה השני $R_p=\mathbb{Z}_p[\alpha]$. במקרה הראשון, אם $p\neq 2$ אז $R_p=\mathbb{Z}_p[\alpha]$.

נותר המקרה הראשון עם $p=2$ ואפשר לקחת $\beta=\frac{1+\sqrt{d}}{2}$ במקום α.

נקח $p\neq 2$, $\alpha=\sqrt{d}$. הפולינום האופייני הוא $f(x)=x^2-d$. יש 3 מקרים

$$PR\quad=\quad\begin{cases}Q_1Q_2 & (f_1=f_2=1)\ \text{completely split}\\ Q & (f_Q=2)\ \text{inert}\\ Q^2 & (f_Q=1)\ \text{ramified}\end{cases}$$

וגם מודולו p

$$x^2-\overline{d}\quad=\quad\begin{cases}(x-\lambda_1)(x-\lambda_2) & (\lambda_1\neq\lambda_2)\\ x^2-\overline{d} & \text{(irreducible)}\\ (x-\lambda)^2 & \end{cases}$$

פירוק מעל $\mathbb{Z}/p\mathbb{Z}$.

המקרה המסועף המקרה של שורש יחיד $x^2-d=(x-\lambda)^2$ ב$\mathbb{Z}/p\mathbb{Z}$. זה קורה $\Longleftrightarrow$ $2\lambda=0\pmod p$ וזה קורה $\Longleftrightarrow$ $\lambda=0\pmod p$ (כי $p\neq 2$). כלומר הפירוק הוא

בעצם
$x^2-d=x^2\pmod p$ ולכן $p\mid d$ והפירוק הוא

$$pR = \left(pR+\sqrt{d}R\right)^2$$

כי $G_1(x)=x$ ולכן $g_1(x)=x$ ו$g_1(\alpha)=\alpha$. ואכן בR מתקיים
$pR\subseteq\left(pR+\sqrt{d}R\right)\subseteq\left(p^2,\sqrt{d}\right)$ ולבסוף $pR=\left(p^2,\sqrt{d}\right)$, כי ב$d$ אין ריבוע.

המקרה inert נניח כי $2\neq p\nmid d$. מקרה זה מתקיים כאשר למשוואה $x^2-d=0$ אין שורשים ב$\mathbb{Z}/p\mathbb{Z}$, כלומר כאשר $\left(\frac{d}{p}\right)=-1$. במקרה זה pR ראשוני.

המקרה split עדיין נניח כי $2\neq p\nmid d$. כאן לd יש שורש מודולו p, כלומר $\left(\frac{d}{p}\right)=1$, ואז אם $n^2=d\pmod p$ נקח $G_{1,2}=x\pm\overline{n}$ ונקח $g_{1,2}=x\pm n$ ואז

$$Q_{1,2} = pR+\left(\sqrt{d}\pm n\right)R$$

ואז

$$\begin{aligned}Q_1Q_2 &= p^2R+p\left(\sqrt{d}+n\right)R+p\left(\sqrt{d}-n\right)R+\left(d-n^2\right)R\\ &\subseteq pR\end{aligned}$$

מצד שני Q_1Q_2 מכיל את $2pn$ ואת p^2 ולכן את $\gcd\left(p^2,2pn\right)=p$ ולכן $Q_1Q_2=pR$.

המקרים בהם $p=2$ אם $d=2,3\pmod 4$ אז $R=\mathbb{Z}\oplus\mathbb{Z}\left[\sqrt{d}\right]$. נבדוק את x^2-d מודולו 2.

- אם $d=2\pmod 4$ אז הפולינום הוא x^2 מודולו 2 ואז $g_1(x)=x$ ומתקבל פירוק

$$2R = \left(2R+\sqrt{d}R\right)^2=\left(2,\sqrt{d}\right)^2$$

ואכן

$$\left(2,\sqrt{d}\right)^2 = \left(4,2\sqrt{d},d\right)=(2)$$

כי d זוגי שאינו מתחלק ב4.

- אם $d=3\pmod 4$ אז הפולינום מודולו 2 הוא $x^2-1=(x+1)^2\pmod 2$. ולכן $g_1(x)=x+1$

$$2R = \left(2,\sqrt{d}+1\right)^2$$

ואכן

$$\left(2,\sqrt{d}+1\right)^2 = \left(4,2\left(\sqrt{d}+1\right),d+2\sqrt{d}+1\right)\subseteq 2R$$

כי d אי־זוגי.
מצד שני אידאל זה מכיל את 4 ואת

$$-2\left(\sqrt{d}+1\right)+\left(d+2\sqrt{d}+1\right) = d-1=2\left(\mod 4\right)$$

ולכן את 2.

נותר המקרה בו $d=1\left(\mod 4\right)$ ו$p=2$. במקרה זה $R=\mathbb{Z}+\frac{1+\sqrt{d}}{2}\mathbb{Z}$. נקח $\beta=\frac{1+\sqrt{d}}{2}$, $N_{K/\mathbb{Q}}\left(\beta\right)=\frac{1-d}{4}$, $\mathrm{Tr}_{K/\mathbb{Q}}\left(\beta\right)=1$ והפולינום האופייני הוא $f\left(x\right)=x^{2}-x+\frac{1-d}{4}$. צריך לבדוק זאת מודולו 2.

במקרה הראשון $d=1\left(\mod 8\right)$: אז f מהצורה $f=x^{2}-x=x\left(x-1\right)\left(\mod 2\right)$ ונקבל

$$\begin{aligned} 2R &= \left(2R+\frac{\sqrt{d}+1}{2}R\right)\left(2R+\left(\frac{\sqrt{d}+1}{2}-1\right)R\right)\\ &= \left(2R+\frac{\sqrt{d}+1}{2}R\right)\left(2R+\left(\frac{\sqrt{d}-1}{2}\right)R\right)\\ &= \left(2,\frac{\sqrt{d}+1}{2}\right)\left(2,\frac{\sqrt{d}-1}{2}\right)\end{aligned}$$

במקרה השני $d=5\left(\mod 8\right)$ אז הפולינום מודולו 2 הוא $x^{2}+x+1$. זהו פולינום אי־פריק מודולו 2 ולכן $2R$ ראשוני.

8.8 הדדיות ריבועית

(מבוסס על Neukirch p.51)

יהי p ראשוני אי־זוגי. יש הומומורפיזם של חבורות כפליות

$$\begin{aligned} s:\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times} &\to \left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}\\ s\left(x\right) &= x^{2}\end{aligned}$$

עם גרעין ±1 ולכן $\left[\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}:\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}\right)^{2}\right]=2$. ויש הומומורפיזם

$$\left\{ n\in\mathbb{Z}\mid p\nmid n\right\} \to\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}\to\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}/\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}\right)^{2} \cong \mathbb{Z}/2\mathbb{Z}\cong\left\{ \pm1\right\} \subseteq\mathbb{Z}$$

ההעתקה הנ"ל היא סמל לז'נדר:

$$\left(p\nmid a\right)\qquad\left(\frac{a}{p}\right)=\begin{cases} 1 & a\text{ is a square }\left(\mod p\right)\\ -1 & \text{else}\end{cases}$$

ומתקיים

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$$

הערה 8.27 קיים c כך ש$\left(\frac{c}{p}\right)=-1$.

יהי $\gamma\in(\mathbb{Z}/p\mathbb{Z})^{\times}$ של $(\mathbb{Z}/p\mathbb{Z})^{\times}$, אז γ מסדר $p-1$. לכל a הזר לp מתקיים $a^{p-1}=1\ (\mod p)$ ולכן $a^{\frac{p-1}{2}}=\pm1\ (\mod p)$.
קיים n כך ש $a=\gamma^{n}\ (\mod p)$. (n נקבע מודולו $p-1$ שהינו זוגי). אז a ריבוע מודולו p $\Longleftrightarrow$ n זוגי $\Longleftrightarrow$ $\frac{n}{2}$ שלם $\Longleftrightarrow$ $p-1\mid\frac{p-1}{2}\cdot n$ $\Longleftrightarrow$ $\gamma^{\frac{p-1}{2}\cdot n}=1\ (\mod p)$ $\Longleftrightarrow$ $a^{\frac{p-1}{2}}=1\ (\mod p)$. לכן

$$\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}\ (\mod p)$$

משפט 8.28 (הדדיות ריבועית): יהיו p,q ראשוניים אי־זוגיים השונים זה מזה. אז

$$\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right)=(-1)^{\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right)}$$

ובנוסף

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$
$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^{2}-1}{8}}$$

הוכחה: השוויון $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ נובע מהשוויון מודולו p. להוכחת הנוסחה הכללית נעבור לחוג $\mathbb{Z}\left[\zeta\right]$ כאשר ζ שורש פרימטיבי של 1 מסדר q.
נסתכל על סכום גאוס:

$$\tau=\sum_{a\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{a}{q}\right)\zeta^{a}\in\mathbb{Z}\left[\zeta\right]$$

נשים לב כי עבור $b\in(\mathbb{Z}/q\mathbb{Z})^{\times}$ מתקיים

$$\left(\frac{b}{q}\right)=\left(\frac{b^{-1}}{q}\right)$$

ולכן

$$\tau=\sum_{b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{b^{-1}}{q}\right)\zeta^{b}$$

כמו כן

$$\sum_{c\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{c}{q}\right)=0$$

כי אם ניקח $t\in(\mathbb{Z}/q\mathbb{Z})^{\times}$ עם $\left(\frac{t}{q}\right)=-1$ אז

$$\begin{aligned}\sum_{c\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{c}{q}\right) &= \sum_{c\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{ct}{q}\right)\\ &= -\sum_{c\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{c}{q}\right)\end{aligned}$$

מכאן נובע $\sum_{1\neq c\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{c}{q}\right)=-1$. נראה ש $\tau^{2}=\left(\frac{-1}{q}\right)q$.

הערה 8.29 בפרט נובע שτ^{2} (ולכן גם τ) אינו מחלק אפס בחוג $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta]$. אחרת היה נובע ש$q$ מחלק אפס, וברור שp מחלק אפס ולכן $\mathbb{Z}[\zeta]=p\mathbb{Z}[\zeta]$, בסתירה לכך ש$\mathbb{Z}[\zeta]$ שלם מעל $\mathbb{Z}$.

נחשב

$$\begin{aligned}\left(\frac{-1}{q}\right)\tau^{2} &= \left(\frac{-1}{q}\right)\sum_{a,b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{ab^{-1}}{q}\right)\zeta^{a+b}\\ &= \sum_{a,b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{a(-b)^{-1}}{q}\right)\zeta^{a+b}\\ &= \sum_{a,b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{ab^{-1}}{q}\right)\zeta^{a-b}\end{aligned}$$

נציב $c=ab^{-1}$:

$$\begin{aligned}\left(\frac{-1}{q}\right)\tau^{2} &= \sum_{c,b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{c}{q}\right)\zeta^{cb-b}\\ &= \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{1}{q}\right)+\sum_{1\neq c\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{c}{q}\right)\sum_{b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\zeta^{b(c-1)}\\ &= (q-1)+\left(\sum_{1\neq c\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{c}{q}\right)\right)\left(\sum_{b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\zeta^{b}\right)\end{aligned}$$

כעת

$$1+\sum_{b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\zeta^{b} = 1+\zeta+\cdots+\zeta^{q-1}=\frac{1-\zeta^{q}}{1-\zeta}=0$$

ולכן

$$\sum_{b\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\zeta^{b} = -1$$

סה"כ

$$\left(\frac{-1}{q}\right)\tau^{2} = (q-1)+(-1)^{2}=q$$

כעת

$$\begin{aligned}\tau^{p} &= \tau\cdot\left(\tau^{2}\right)^{\frac{p-1}{2}}\\ &= \tau\cdot\left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\cdot q^{\frac{p-1}{2}}\\ &= \tau\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot q^{\frac{p-1}{2}}\\ &\equiv \tau\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right)\left(\mod p\mathbb{Z}\left[\zeta\right]\right)\end{aligned}$$

מצד שני מודולו p מתקיים

$$\begin{aligned}\tau^{p} &\equiv \sum_{a\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{a}{q}\right)^{p}\zeta^{ap}\left(\mod p\mathbb{Z}\left[\zeta\right]\right)\\ &\equiv \sum_{a\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{a}{q}\right)\zeta^{ap}\left(\mod p\mathbb{Z}\left[\zeta\right]\right)\\ &= \left(\frac{p}{q}\right)\cdot\sum_{a\in(\mathbb{Z}/q\mathbb{Z})^{\times}}\left(\frac{ap}{q}\right)\zeta^{ap}\\ &= \left(\frac{p}{q}\right)\tau\end{aligned}$$

כאשר השוויון האחרון נכון כי p זר לq. בסה"כ קיבלנו כי

$$\tau\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right) \equiv \left(\frac{p}{q}\right)\tau\left(\mod p\mathbb{Z}\left[\zeta\right]\right)$$

ראינו שτ לא מחלק אפס בחוג $\mathbb{Z}\left[\zeta\right]/p\mathbb{Z}\left[\zeta\right]$ ולכן ניתן לחלק בτ וע"י כפל ב$\left(\frac{q}{p}\right)$ נקבל

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)$$

לגבי $\left(\frac{2}{p}\right)$: נעבוד בחוג השלמים של גאוס $\mathbb{Z}\left[i\right]$. מתקיים $(i+1)^{2}=2i$ ולכן

$$\begin{aligned}(1+i)^{p} &= (1+i)\left((1+i)^{2}\right)^{\frac{p-1}{2}}\\ &= (1+i)\,(2i)^{\frac{p-1}{2}}\\ &= (1+i)\,2^{\frac{p-1}{2}}i^{\frac{p-1}{2}}\end{aligned}$$

הערה 8.30 2 הוא לא מחלק אפס ב$\mathbb{Z}[i]/p\mathbb{Z}[i]$ כי p אי־זוגי (ואז גם p מחלק אפס ומכאן $\mathbb{Z}[i]=p\mathbb{Z}[i]$) ואז מתוך $2=(1-i)(1+i)$ נובע ש$1\pm i$ אינם מחלקי אפס בחוג זה.

מהשוויון לעיל מסיקים

$$\begin{aligned}
1+i(-1)^{\frac{p-1}{2}} &= 1+i^p \\
&\equiv (1+i)^p \pmod{p\mathbb{Z}[i]} \\
&\equiv (1+i)\left(\frac{2}{p}\right)i^{\frac{p-1}{2}} \pmod{p\mathbb{Z}[i]}
\end{aligned}$$

אם $\frac{p-1}{2}$ זוגי, נסיק ש

$$1+i \equiv (1+i)\left(\frac{2}{p}\right)\cdot(-1)^{\frac{p-1}{4}}$$

ולכן

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{4}}=(-1)^{\frac{p^2-1}{8}}$$

כי $\frac{p+1}{2}$ אי־זוגי ו$\left(\frac{p-1}{4}\right)\cdot\left(\frac{p+1}{2}\right)=\frac{p^2-1}{8}$.

אם $\frac{p-1}{2}$ אי־זוגי, אז

$$\begin{aligned}
1+i(-1)^{\frac{p-1}{2}} &= 1-i \\
&\equiv (1+i)\left(\frac{2}{p}\right)i^{\frac{p-1}{2}} \pmod{p\mathbb{Z}[i]} \\
&= (1+i)\left(\frac{2}{p}\right)\frac{i^{\frac{p+1}{2}}}{i} \\
&= (1-i)\left(\frac{2}{p}\right)i^{\frac{p+1}{2}}
\end{aligned}$$

ולכן

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}=(-1)^{\frac{p^2-1}{8}}$$

כי $\frac{p-1}{4}$ אי־זוגי ו

$$\frac{p-1}{2}\cdot\frac{p+1}{4} = \frac{p^2-1}{8}$$

■

9 הערכות על שדות

9.1 ערכים מוחלטים

למה 9.1 יהי K שדה. תהי $|\cdot|:K\to[0,\infty)$ פונקציה המקיימת

1. חיוביות: $|x| = 0 \iff x = 0$
2. כפליות $|x \cdot y| = |x| \cdot |y|$

אז התנאים הבאים השקולים:

- (אי־שוויון המשולש) $|x + y| \leq |x| + |y|$
- $|x + y| \leq 2\max(|x|, |y|)$

הערה 9.2 מכפליות נובע $|1| \cdot |1| = |1|$ ומחיוביות נובע $|1| \neq 0$ ולכן $|1| = 1$. באופן זהה $|-1| = 1$.

הגדרה 9.3 אם התנאים השקולים של הלמה מתקיימים, אומרים ש־$|\cdot|$ ערך מוחלט על K.

הוכחה: (של הלמה): ברור כי אי־שוויון המשולש $\Longleftarrow$ $|x + y| \leq 2\max(x, y)$.

בכיוון ההפוך: נניח כי $|x + y| \leq 2\max(x, y)$. ראשית נראה באינדוקציה כי לכל $k \geq 0$ מתקיים $|a_1 + \cdots + a_{2^k}| \leq 2^k \cdot \max_{i=1}^{k} |a_i|$. עבור $k = 0, 1$ זה ברור. נניח כי זה נכון ל־k ונוכיח עבור $k + 1$:

$$\begin{aligned}
|a_1 + \cdots + a_{2^{k+1}}| &= |(a_1 + \cdots + a_{2^k}) + (a_{2^k+1} \cdots + a_{2^{k+1}})| \\
&\leq 2\max(|a_1 + \cdots + a_{2^k}|, |a_{2^k+1} \cdots + a_{2^{k+1}}|) \\
&\leq 2\max\left(2^k \max_{i=1}^{2^k} |a_i|, 2^k \max_{i=2^k+1}^{2^{k+1}} |a_i|\right) \\
&= 2^{k+1} \max_{i=1}^{2^{k+1}} |a_i|
\end{aligned}$$

כנדרש.

לכן לכל $n = 1, 2, \ldots$ מתקיים

$$|a_1 + \cdots + a_n| \leq 2n \cdot \max_{i=1}^{n} |a_i|$$

כי יהי $2^k \leq n \leq 2^{k+1}$ אז

$$\begin{aligned}
|a_1 + a_2 + \cdots + a_n| &\leq 2^{k+1} \cdot \max_{i=1}^{n} |a_i| \\
&\leq 2n \cdot \max_{i=1}^{n} |a_i|
\end{aligned}$$

בפרט נובע $|n| = \left|\underbrace{1+1+\cdots+1}_{n\text{ times}}\right| \leq 2n$ ולכן

$$\begin{aligned} |x+y|^n &= |(x+y)^n| \\ &= \left|\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\right| \\ &\leq 2(n+1)\cdot\sum_{k=0}^{n}\left|\binom{n}{k}\right||x|^k|y|^{n-k} \\ &\leq 2(n+1)\cdot\sum_{k=0}^{n}2\binom{n}{k}|x|^k|y|^{n-k} \\ &= 4(n+1)\sum_{k=0}^{n}\binom{n}{k}|x|^k|y|^{n-k} \\ &= 4(n+1)(|x|+|y|)^n \end{aligned}$$

לכן (ע"י הוצאת שורש nי משני האגפים)

$$|x+y| \quad\leq\quad \sqrt[n]{4(n+1)}\cdot(|x|+|y|) \underset{n\to\infty}{\longrightarrow} |x|+|y|$$

■

9.2 הערכות

יהי K שדה. שתי פונקציות $f,g : K \to [0,\infty)$ נקראות שקולות אם קיים $\rho > 0$ כך ש$f(x) = g(x)^\rho$ (לכל $x \in K$).

הערה 9.4 התנאים "חיוביות" ו"כפליות" אינווריאנטיים לשקילות.

הגדרה 9.5 $|\cdot| : K \to [0,\infty)$ נקראת הערכה (על K) אם היא שקולה לערך מוחלט. כלומר $|\cdot|$ נדרש לקיים חיוביות, כפליות ו

- קיים $\rho > 0$ כך ש$|x+y|^\rho \leq |x|^\rho + |y|^\rho$.

לאור הלמה, בהנתן חיוביות וכפליות, התנאי הזה שקול לכך שקיים $A \geq 0$ כך ש $|x+y| \leq A\cdot\max(|x|,|y|)$.

הערה 9.6 תנאי שקול נוסף בהנתן חיוביות וכפליות, הוא: קיים $A \geq 0$ כך ש $\sup_{|x|\leq 1}|x+1| \leq A$ (מניחים כי $0 \neq |y| \geq |x|$ ואז $\left|1+\frac{x}{y}\right| \leq A$ ומכפילים ב$|y|$)

הערה 9.7 נובע $A \geq 1$ (ע"י $x = 1$ ו$y = 0$).

9.3 הטופולוגיה המוגדרת ע"י הערכה

יהי $(K,|\cdot|)$ שדה הערכה.

הגדרה 9.8 לכל $X\subseteq K$ נאמר שX פתוחה אם לכל $x\in X$ קיים $\varepsilon>0$ כך ש

$$B^{|\cdot|}(x,\varepsilon) = \{y\in K \mid |x-y|<\varepsilon\}\subseteq K$$

הערה 9.9 אם $|\cdot|,|\cdot|'$ הערכות שקולות, יש להן אותן קבוצות פתוחות.

מסקנה 9.10 לתיאור הקבוצות הפתוחות, אפשר להניח ש$|\cdot|$ היא ערך מוחלט. במקרה זה $|\cdot|$ מגדירה מטריקה ע"י $d(x,y)=|x-y|$. (הסימטריות נובעות מכך ש$|-1|=1$ ומכפליות) לכן הקבוצות הפתוחות מהוות טופולוגיה על K וטופולוגיה זו היא מטרית.

הערה 9.11 במצב זה הטופולוגיה לעיל הופכת את K לשדה טופולוגי, כלומר הפונקציות

$$\begin{aligned} +:K\times K &\to K \\ \cdot:K\times K &\to K \end{aligned}$$

ופונקציית ההופכי

$$\begin{aligned} K^{\times} &\to K^{\times} \\ x &\mapsto x^{-1} \end{aligned}$$

הן רציפות.

הוכחה: די לבדוק במקרה בו $|\cdot|$ ערך מוחלט, ובמקרה זה ההוכחה כרגיל. ■

מסקנה 9.12 הפונקציות $x\mapsto a+x$ וכפל בבסקלר $b\neq 0$ השונה מאפס $x\mapsto b\cdot x$ הם הומיאומורפיזמים.

הערה 9.13

1. הפונקציה $K\times K\to\mathbb{R}$, $(x,y)\mapsto|x-y|$ היא רציפה. (כי פונקציית המרחק רציפה בכל מרחב מטרי)
2. בפרט $|\cdot|:K\to\mathbb{R}$, $x\mapsto|x|$ רציפה.
3. $\lim_{n\to\infty}x^n=0 \iff \lim_{n\to\infty}|x^n-0|=0 \iff \lim_{n\to\infty}|x|^n=0 \iff |x|<1$
4. אומרים ש$|\cdot|$ <u>לא טריוואלי</u> אם קיים $0\neq x\in K$ כך ש$|x|\neq 1$ ואז $|x|<1$ או $|x|>1$ ובהתאמה $\left|x^{-1}\right|>1$ או $\left|x^{-1}\right|<1$.

9.4 שקילות וטופולוגיה

טענה 9.14 תהיינה $|\cdot|, |\cdot|'$ שתי הערכות לא טריוואליות. התנאים הבאים שקולים:

1. $|\cdot|, |\cdot|'$ שקולות
2. $|\cdot|, |\cdot|'$ מגדירות אותה טופולוגיה
3. פונקציית הזהות $\mathrm{id} : (K, |\cdot|) \to (K, |\cdot|')$ רציפה
4. $|x| < 1 \implies |x|' < 1$
5. $|x| \le 1 \implies |x|' \le 1$
6. $\begin{cases} |x| < 1 & \iff |x|' < 1 \\ |x| = 1 & \iff |x|' = 1 \\ |x| > 1 & \iff |x|' > 1 \end{cases}$

הוכחה: $1 \Longleftarrow 2 \Longleftarrow 3 \Longleftarrow 4$ מיידי מההערה.
$5 \implies 4$: יהי $b \in K^\times$ עם $0 < |b| < 1$. אז אם $|x| \le 1$ אז לכל $n \ge 1$ מתקיים $|x^n b| = |x^n| |b| \le |b| < 1$ ולכן $|x^n b|' < 1$ ומכאן $|x^n b|' = \left(|x|'\right)^n |b|' < 1$. נוציא שורש nי ונקבל

$$|x|' < \sqrt[n]{\frac{1}{|b|'}}$$

וע"י לקיחת גבול נקבל $|x|' \le \lim_{n\to\infty} \sqrt[n]{\frac{1}{|b|'}} = 1$.
$6 \implies 5$: נקח $c \in K^\times$ עם $0 < |c|' < 1$. יהי $|x| < 1$ אז קיים n כך ש

$$\begin{array}{ccc} \left|\frac{x^n}{c}\right| & = & \frac{|x|^n}{|c|} \le 1 \\ & \implies & \\ \frac{|x|'^n}{|c|'} & \le & 1 \\ & \implies & \\ |x|'^n & \le & |c|' < 1 \\ & \implies & \\ |x|' & < & 1 \end{array}$$

לכן $|x| < 1 \implies |x|' < 1$. מכאן אם $|x| > 1$ אז $\left|x^{-1}\right| < 1$ ולכן $\left|x^{-1}\right|' < 1$ ומכאן $1 < |x|'$.
לבסוף אם $|x| = 1$ אז $\left|x^{\pm 1}\right| \le 1$ ולכן $\left|x^{\pm 1}\right|' \le 1$ ומכאן $|x|' = 1$.
לבסוף הראנו כי $\begin{cases} |x| < 1 & \implies |x|' < 1 \\ |x| = 1 & \implies |x|' = 1 \\ |x| > 1 & \implies |x|' > 1 \end{cases}$ וזה מספיק. (למשל אם $|x|' < 1$ לא ייתכן $|x| \ge 1$ כי אז $|x|' \ge 1$, וכו')

$1 \impliedby 6$: נקח $a\in K$ עם $|a|>1$ ואז $|a|'>1$. נראה כי לכל $x\in K^{\times}$ מתקיים

$$\frac{\log|x|}{\log|a|} = \frac{\log|x|'}{\log|a|'}$$

אכן, יהי $r=\frac{m}{n}$ רציונלי עם $n>0$. אז

$$\begin{aligned}
r &\geq \frac{\log|x|}{\log|a|}\\
&\Longleftrightarrow\\
m\log|a| &\geq n\log|x|\\
\log|a|^m &\geq \log|x|^n\\
\log|a^m| &\geq \log|x^n|\\
&\Longleftrightarrow\\
\log\left|\frac{a^m}{x^n}\right| &\geq 0\\
&\Longleftrightarrow\\
\left|\frac{a^m}{x^n}\right| &\geq 1\\
&\Longleftrightarrow\\
\left|\frac{a^m}{x^n}\right|' &\geq 1\\
&\Longleftrightarrow\\
r &\geq \frac{\log|x|'}{\log|a|'}
\end{aligned}$$

לכן $\frac{\log|x|'}{\log|a|'}=\frac{\log|x|}{\log|a|}$ (אחרת קיים מספר רציונלי ביניהם). נסמן $\rho=\frac{\log|a|'}{\log|a|}$. אז לכל $x\in K^{\times}$ מתקיים

$$\log|x|' = \rho\log|x|$$

כלומר $|x|'=|x|^{\rho}$ כנדרש. ■

9.5 משפט קירוב חלש

הערה 9.15 אם $(K,|\cdot|)$ שדה הערכה אז עבור $b\in K$:

- אם $|b|<1$ אז

$$\lim_{n\to\infty}\frac{b^n}{1+b^n} = \frac{0}{1+0}=0$$

- אם $|b|>1$ אז

$$\lim_{n\to\infty}\frac{b^n}{1+b^n} = \lim_{n\to\infty}\frac{1}{\frac{1}{b^n}+1}=\frac{1}{1+0}=1$$

משפט 9.16 תהיינה $|\cdot|_1, \ldots, |\cdot|_n$ הערכות לא טריוואליות של שדה K שאינן שקולות אחת לשנייה, ויהיו $a_1, \ldots, a_n \in K$ ו$\varepsilon > 0$. אז קיים $x \in K$ כך ש

$$|x - a_i|_i < \varepsilon \qquad (\forall 1 \leq i \leq n)$$

הערה 9.17 (תיאור נוסף של המשפט): באותם תנאים, קיימת סדרה $\{x_l\}_{l=1}^{\infty}$ כך שלפי הטופולוגיה של $|\cdot|_i$ (כאשר $i = 1, \ldots, n$) מתקיים

$$x_l \quad \underset{l \to \infty}{\longrightarrow} \quad a_i$$

הוכחת המשפט לפי ההוכחה בWeiss. נתחיל ראשית עם למות:

למה 9.18 באותם סימונים, קיים $a \in K$ כך ש

$$|a|_1 > 1, |a|_2 < 1, \quad \ldots \quad |a|_n < 1$$

הוכחה: באינדוקציה על n. עבור $n = 2$: מהטענות הקודמות (על שקילות הערכות) קיימים $b, c \in K$ כך ש

$$\begin{array}{ll} |b|_1 < 1 & \quad |b|_2 \geq 1 \\ |c|_1 \geq 1 & \quad |c|_2 < 1 \end{array}$$

בפרט $b \neq 0$ ואז

$$\left|\frac{c}{b}\right|_2 < 1 \qquad \left|\frac{c}{b}\right|_1 > 1$$

ולכן $a = \frac{c}{b}$ עונה על הדרוש.
נניח $n \geq 3$ ושהוכחנו ל$n - 1$. קיים $b \in K$ כך ש

$$|b|_1 > 1, |b|_2 < 1, \quad \ldots \quad |b|_{n-1} < 1$$

לפי המקרה $n = 2$ ניתן למצוא $c \in K$ כך ש$|c|_1 > 1$ ו$|c|_n < 1$. אם $|b|_n \leq 1$ אפשר לקחת $a = b^k c$ עבור k גדול דיו. אם $|b|_n > 1$, אפשר לקחת $a = \frac{b^k}{1+b^k} c$ עבור k גדול דיו.
■

למה 9.19 באותם סימונים, לכל $\varepsilon > 0$ יש $b \in K$ כך ש

$$|b - 1|_1 < \varepsilon, |b|_2 < \varepsilon, \quad \ldots \quad |b|_n < \varepsilon$$

הוכחה: נקח a כמו בלמה הקודמת ונקח $b = \frac{a^k}{1+a^k}$ עבור k גדול דיו. ■

מסקנה 9.20 לכל $j=1,\ldots,n$ קיימת סדרה $\{b_{jl}\}_{l=1}^{\infty}$ כך ש$b_{jl}\underset{l\to\infty}{\longrightarrow}0$ לפי הטופולוגיה $|\cdot|_i$ כאשר $j \neq i$ ו$b_{jl}\underset{l\to\infty}{\longrightarrow}1$ לפי הטופולוגיה $|\cdot|_j$.
נעבור להוכחת המשפט.

הוכחה: נסמן $x_l = \sum_{j=1}^{n} b_{jl}a_j$ אז לפי הטופולוגיה של $|\cdot|_i$ מתקיים $x_l\underset{l\to\infty}{\longrightarrow}a_i$, ונקח $x = x_l$ עם l גדול דיו. ■

9.6 הערכות ארכימדיות ולא ארכימדיות

הגדרה 9.21 יהי K שדה ותהי $|\cdot| : K \to [0,\infty)$ פונקציה המקיימת

- (חיוביות): $|x| = 0 \iff x = 0$
- (כפליות): $|xy| = |x| \cdot |y|$

אם $|\cdot|$ מקיימת גם $|x+y| \leq \max\{|x|,|y|\}$ ("אי־שוויון לא ארכימדי") אז $|\cdot|$ נקראת הערכה לא ארכימדית.

הערה 9.22

1. ברור שנובע $|x+y| \leq |x| + |y|$ ולכן $|\cdot|$ ערך מוחלט ובפרט הערכה.
2. אם $|\cdot|, |\cdot|' : K \to [0,\infty)$ שקולות, אז $|\cdot|$ הערכה לא ארכימדית $\iff$ $|\cdot|'$ הערכה לא ארכימדית.

הגדרה 9.23 הערכה $|\cdot|$ על שדה K שאינה לא ארכימדית, נקראת ארכימדית. כלומר נדרשת לקיים:

- (חיוביות): $|x| = 0 \iff x = 0$
- (כפליות): $|xy| = |x| \cdot |y|$
- (שקולה לערך מוחלט): קיים α כך ש$|x+y|^{\alpha} \leq |x|^{\alpha} + |y|^{\alpha}$
- קיימים $x_0, y_0 \in K$ כך ש$|x_0 + y_0| > \max\{|x_0|,|y_0|\}$

הערה 9.24 (דוגמה): הערך מוחלט הרגיל על $\mathbb{Q}$.

9.7 תכונות מיידיות של הערכות לא ארכימדיות

1. $|\pm x_1 \pm x_2 \pm \cdots \pm x_n| \leq \max\{|x_1|,\ldots,|x_n|\}$
2. אם $|y| < |x|$ אז $|\pm x \pm y| = |x|$ כי $|\pm x \pm y| \leq \max\{|x|,|y|\}$ ואילו היה $|\pm x \pm y| < |x|$ אז היינו מקבלים

$$\begin{aligned} |x| &= |\pm x| \\ &= |\pm x \pm y \mp y| \\ &\leq \max(|\pm x \pm y|,|y|) < |x| \end{aligned}$$

סתירה.

3. כל המשולשים הם שווי צלעות או שווי שוקיים, ובמקרה השני הצלע "השונה" היא הצלע הקטנה.

4. אם $|x_1| > |x_2|, \ldots, |x_1| > |x_n|$ אז

$$|\pm x_1 \pm x_2 \pm \cdots \pm x_n| \quad = \quad |x_1|$$

5. אם $\lim_{n\to\infty} a_n = a \neq 0$ אז קיים N כך שעבור $n > N$ מתקיים $|a_n| = |a|$ - ואכן די לקחת $|a_n - a| < |a|$.

9.8 איפיון הערכות לא ארכימדיות

יהי K שדה. לכל $n = 0, 1, 2, \ldots$

$$K \ni n \quad = \quad \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$

טענה 9.25 תהי $|\cdot|$ הערכה על שדה, אז $|\cdot|$ לא ארכימדית, אם ורק אם $\sup_{n=1,2,\ldots} |n| < \infty$ (ובמקרה זה $|n| \leq 1$ לכל $n \in \mathbb{Z}$)

מסקנה 9.26

1. אם המציין של K חיובי, אז $|\cdot|$ לא ארכימדית.

2. תהי K/F הרחבת שדות ו$|\cdot|$ הערכה של K, $|\cdot|_F$ הצמצום על F (גם זו הערכה). אז $|\cdot|$ לא ארכימדית $\iff$ $|\cdot|$ לא ארכימדית.

נוכיח את הטענה. **הוכחה:** התנאים אינווראינטיים לשקילות, לכן אפשר להניח כי $|\cdot|$ ערך מוחלט.

אם $|\cdot|$ אינה ארכימדית, ברור ש $|n| = |1 + 1 + \cdots + 1| \leq \max\{|1|, \ldots, |1|\} = 1$.

בכיוון ההפוך: נניח שקיים $C > 0$ כך שלכל $n = 1, 2, \ldots$ מתקיים $|n| \leq C$. לכל $a, b \in K$ מתקיים

$$\begin{aligned}
|a+b|^n &= |(a+b)^n| \\
&= \left|\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}\right| \\
&\leq \sum_{i=0}^{n} \left|\binom{n}{i}\right| |a|^i |b|^{n-i} \\
&\leq C \cdot \sum_{i=0}^{n} |a|^i |b|^{n-i} \\
&\leq C \cdot (n+1) \cdot \max(|a|, |b|)^n
\end{aligned}$$

נוציא שורש nי ונקבל

$$|a+b| \quad \leq \quad \sqrt[n]{C} \cdot \sqrt[n]{n+1} \cdot \max(|a|, |b|)$$

ניקח גבול כאשר $n \longrightarrow \infty$ ונקבל $|a+b| \leq \max(|a|, |b|)$, כנדרש. ■

9.9 $\mathbb{Q}$

טענה 9.27 על $\mathbb{Q}$ ישנן ההערכות הבאות:

1. הערכה ארכימדית: הערך המוחלט הרגיל $|\cdot|_\infty$
2. לכל מספר ראשוני p ישנה הערכה לא ארכימדית המסומנת $|\cdot|_p$ ונתונה ע"י

$$\left|\frac{a}{b}p^n\right| = \frac{1}{p^n}$$

כאשר $a,b\neq 0$ שלמים הזרים ל-p, $n\in\mathbb{Z}$.

וכל הערכה על $\mathbb{Q}$ שקולה לאחת מההערכות האלה, והערכות אלה אינן שקולות אחת לשנייה.

הוכחה: מאחר והראנו כי אין הערכה שהיא גם ארכימדית וגם לא־ארכימדית, נחלק את ההוכחה לשני חלקים:

הערכות לא ארכימדיות: נבדוק ש-$|\cdot|_p$ הערכה לא ארכימדית. חיוביות ברורה, כפליות ברורה, ונוכיח את אי־שוויון המשולש הלא ארכימדי. יהיו $x=p^n\cdot\frac{a}{b}$ ו-$y=p^k\cdot\frac{c}{d}$ עם a,b,c,d הזרים ל-p. נניח בלי הגבלת הכלליות כי $n\geq k$. אז

$$\begin{aligned} |x+y|_p &= \left|p^k\left(p^{n-k}\frac{a}{b}+\frac{c}{d}\right)\right|_p \\ &= \left|p^k\right|_p\cdot\left|\frac{p^{n-k}ad+bc}{bc}\right|_p \\ &\leq \frac{1}{p^k}\cdot 1=\max\left(\frac{1}{p^n},\frac{1}{p^k}\right)=\max\left(|x|_p,|y|_p\right)\end{aligned}$$

בכיוון ההפוך: תהי $|\cdot|$ הערכה לא ארכימדית על $\mathbb{Q}$. אז $|n|\leq 1$ (לכל $n\in\mathbb{Z}$). נסמן

$$P = \{n\in\mathbb{Z}\mid |n|<1\}$$

אז $P\subseteq\mathbb{Z}$ אידאל ראשוני ו-$P\neq 0$, כי אחרת היה $|n|=1$ לכל n ולכן $|x|=1$ לכל $x\in\mathbb{Q}$ ולכן $|\cdot|$ טריוואלי. סתירה. $P\neq\mathbb{Z}$ כי $|1|=1$ ולכן $1\notin P$.

יהי $p>0$ היוצר הראשוני של P. אם $(n,p)=1$ אז $|n|=1$ (אחרת $n\in P$ ואז $P=\mathbb{Z}$ - סתירה). לכן אם $a,b\neq 0$ זרים ל-p אז

$$\left|p^n\cdot\frac{a}{b}\right| = |p|^n$$

מאחר ו-$|p|<1$, אפשר ע"י מעבר להערכה שקולה להניח כי $|p|=\frac{1}{p}$ ולכן $|\cdot|_p=|\cdot|$. לבסוף ההערכות $\left\{|\cdot|_p \mid p \text{ is prime}\right\}$ אינן שקולות, לפי הטענה על תנאים שווים לשקילות.

הערכות ארכימדיות: תהי $|\cdot|$ הערכה ארכימדית על $\mathbb{Q}$, מניחים ש-$|\cdot|$ ערך מוחלט. יהיו $m,n>1$ טבעיים. לכל t טבעי יש פיתוח

$$m^t = a_sn^s+\cdots+a_1n+a_0$$

כאשר $0\leq a_i<n$ ו-$a_s\neq 0$. אז $n^s\leq m^t$. מאחר ש

$$|a_i| \leq a_i<n$$

(מאי־שוויון המשולש) נקבל

$$\begin{aligned}|m|^{t} &= \left|m^{t}\right|\\ &\leq |a_s|\cdot|n|^{s}+\cdots+|a_0|\\ &\leq n\cdot\left(|n|^{s}+\cdots+1\right)\\ &\leq n\cdot(s+1)\cdot\max\left(1,|n|\right)^{s}\\ &\leq n\left(t\frac{\log m}{\log n}+1\right)\cdot\max\left(1,|n|\right)^{t\frac{\log m}{\log n}}\end{aligned}$$

נוציא שורש t ונשאיף את t לאינסוף ונקבל

$$|m| \leq \sqrt[t]{n}\sqrt[t]{\left(t\frac{\log m}{\log n}+1\right)}\cdot\max\left(1,|n|\right)^{\frac{\log m}{\log n}} \underset{t\to\infty}{\longrightarrow} \max\left(1,|n|\right)^{\frac{\log m}{\log n}}$$

מסקנה 9.28 לכל $n>1$ מתקיים $|n|>1$ - אחרת היה נובע $|m|\leq 1$ לכל $m>1$ ולכן לכל $m\geq 1$ ואז $|\cdot|$ לא ארכימדית. סתירה.

מכאן $|m|\leq|n|^{\frac{\log m}{\log n}}$ לכל $m,n>1$ ולכן $|n|^{\frac{1}{\log n}}=|m|^{\frac{1}{\log m}}$ ערך משותף לכל $m,n>1$. ערך משותף זה גדול מ1. נסמן

$$e^{\rho}=|n|^{\frac{1}{\log n}} \qquad (n>1)$$

אז $\rho>0$ ומתקיים

$$|n| = e^{\rho\log n}=n^{\rho}=|n|_{\infty}^{\rho}$$

מתקיים גם $|\pm1|_{\infty}^{\rho}=1=|\pm1|$ ולכן מכפליות נובע $|\cdot|=|\cdot|_{\infty}^{\rho}$. ■

9.10 קבועים אופטימליים

הגדרה 9.29 (סימון): תהי $|\cdot|:K\to[0,\infty)$ הערכה על שדה K. אז קיים $A\geq 0$ כך ש$|x+y|\leq A\cdot\max\left(|x|,|y|\right)$ (ואז $A\geq 1$). נסמן

$$C_{|\cdot|} = \min\left\{A\geq 0 \mid |x+y|\leq A\cdot\max\left\{|x|,|y|\right\}(\forall x,y\in K)\right\}$$

אז $|x+y|\leq C_{|\cdot|}\max\left(|x|,|y|\right)$ (לכל $x,y\in K$) ו$C_{|\cdot|}$ המספר הקטן ביותר עם תכונה זאת.

הערה 9.30 $|\cdot|$ ערך מוחלט $\iff$ $C_{|\cdot|}\leq 2$.

טענה 9.31 $C_{|\cdot|}=\max\left\{1,|2|\right\}$

הוכחה: ע"י הצבת $x=1,y=0$ נוכיח $C_{|\cdot|}\geq 1$. ע"י הצבת $x=y=1$ נקבל $C_{|\cdot|}\geq|2|$. לכן $C_{|\cdot|}\geq\max\left\{1,|2|\right\}$. נותר להוכיח כי

$$|x+y|\leq\max\left\{1,|2|\right\}\cdot\max\left\{|x|,|y|\right\} \qquad (x,y\in K)$$

אם $|\cdot|$ לא ארכימדי זה נכון. לכן אפשר להניח ש$|\cdot|$ ארכימדית. זה נובע מהלמה הבאה:

למה 9.32 אם $|\cdot|$ הערכה ארכימדית על שדה K אז $|x+y| \leq |2| \cdot \max(|x|,|y|)$ לכל $x,y \in K$.

הוכחה: האי־שוויון אינווריאנטי ביחס לשקילות המעבירה את $|\cdot|$ ל־$|\cdot|^{\rho}$ (ל־$\rho > 0$). לכן אפשר להניח ש־$|\cdot|$ ערך מוחלט. כעת הצמצום של $|\cdot|$ על $\mathbb{Q}$ ארכימדי ולכן שקול ל־$|\cdot|_{\infty}$, כלומר קיים $\rho > 0$ כך ש־$|x| = |x|_{\infty}^{\rho}$ לכל $x \in \mathbb{Q}$ ($\mathrm{char}K = 0$ כי $|\cdot|$ ארכימדית).

לכל $x,y \in K$ ו־$n = 1,2,\ldots$ מתקיים

$$\begin{aligned} |x+y|^n &= |(x+y)^n| \\ &= \left|\sum_{i=0}^{n}\binom{n}{i}\cdot x^i y^{n-i}\right| \\ &\leq \sum_{i=0}^{n}\left|\binom{n}{i}\right|_{\infty}^{\rho}\cdot\max(|x|,|y|)^n \\ &\leq (n+1)\,|2|_{\infty}^{n\rho}\cdot\max(|x|,|y|)^n \end{aligned}$$

נוציא שורש n־י ונשאיף את n לאינסוף ונקבל

$$\begin{aligned} |x+y| &\leq \sqrt[n]{n+1}\cdot|2|_{\infty}^{\rho}\cdot\max(|x|,|y|) \underset{n\to\infty}{\longrightarrow} \underbrace{|2|_{\infty}^{\rho}}_{|2|}\cdot\max(|x|,|y|) \\ |x+y| &\leq |2|\cdot\max(|x|,|y|) \end{aligned}$$

כנדרש. ■

■

מסקנה 9.33

1. תהי $|\cdot|$ הערכה על K. אם $|2| \leq 2$ אז $|\cdot|$ ערך מוחלט, ואם $|2| > 2$ אז $|\cdot|$ לא ערך מוחלט.
2. תהי $|\cdot|$ הערכה ארכימדית. עבור $\rho > 0$, $|\cdot|^{\rho}$ היא ערך מוחלט אם ורק אם $|2|^{\rho} \leq 2$.
3. אם K שדה עם מציין 0 (ואז $\mathbb{Q} \subseteq K$) ואם $|\cdot|$ הערכה על K כך שהצמצום של $|\cdot|$ על $\mathbb{Q}$ הינו הערך המוחלט ה"רגיל", אז $|\cdot|$ היא ערך מוחלט (כי $|2| = |2|_{\infty} = 2$).

9.11 שלמים בשדה הערכה לא ארכימדי

תהי $|\cdot|$ הערכה לא ארכימדית על שדה K. נסמן

$$R = \{x \in K \mid |x| \leq 1\}$$

"חוג השלמים", "חוג ההערכה".

$$U = \{x \in K \mid |x| = 1\}$$

$R^{\times} = U$ כלומר ההפיכים.

$$P = \{x \in K \mid |x| < 1\}$$

האידאל המקסימלי (היחיד של R). ייצוג נוסף

$$P = \left\{x\in K \mid \lim_{n\to\infty} x^n = 0\right\}$$

מסקנה 9.34 אם $\varphi : K \to K$ אוטומורפיזם אלגברי והומיאומורפיזם, אז φ שומר את R, U ו־P.

הוכחה: אכן $K = R\cup(P\setminus\{0\})^{-1}$ ו־φ כנ"ל, מעביר $x\in P$ ל־$\varphi(x)$ עם $\varphi(x)^n = \varphi(x^n) \underset{n\to\infty}{\longrightarrow} 0$. ■

טענה 9.35 P, U, R תת־קבוצות פתוחות וסגורות של K.

הוכחה: אכן

$$P = \text{Open Ball}^{|\cdot|}(0,1)$$

פתוחה כמו בכל מרחב מטרי. מאחר ש־P תת־חבורה של $\langle K,+\rangle$ נובע ש־P גם סגורה. (כי K איחוד של קוסטים של P והן כולן פתוחות, ולכן המשלים של P פתוח)

לבסוף U סגורה כמו בכל מרחב מטרי ו־U פתוחה כי $U = U+P$ (ניתן לכתיבה כאיחוד של קוסטים של P שכולן פתוחות). ■

טענה 9.36 K הוא שדה המנות של R, ולמעשה מתקיים התנאי $K = R\cup(P\setminus\{0\})^{-1}$ היותר חזק.

טענה 9.37 R סגור בשלמות.

הוכחה: נניח כי $x\in K$ מקיים משוואה מהצורה

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

עם $a_i\in R$ לכל i. אילו היה $|x|>1$ היינו מקבלים

$$\begin{aligned} |x|^n &= |x^n| \\ &= \left|a_{n-1}x^{n-1}+\cdots+a_0\right| \le |x|^{n-1} \end{aligned}$$

כלומר $|x|\le 1$. סתירה. לכן $|x|\le 1$, כלומר $x\in R$. ■

9.12 שדה שארית

תהי $|\cdot|$ הערכה לא ארכימדית על שדה K. מסמנים $\overline{K} = R/P$ - נקרא שדה השארית. יש הומומורפיזם של חוגים:

$$\begin{aligned} \bar{\cdot} : R &\to \overline{K} = R/P \\ x &\mapsto \overline{x} = x+P \end{aligned}$$

ומתקיים

$$\overline{x} = \overline{y} \iff |x-y| < 1$$

כאשר $x,y\in R$.

הגדרה 9.38 (מינוח): קבוצת נציגים היא קבוצה $R \subseteq \{x_i\}_{i\in I}$ כך ש $\overline{K} = \{\overline{x_i}\}_{i\in I}$ ו$\overline{x_i} \neq \overline{x_j}$ עבור $i \neq j$ כלומר ההעתקה

$$\{x_i\}_{i\in I} \to \overline{K} \qquad x_i \mapsto \overline{x_i}$$

היא חד־חד־ערכית ועל.

הערה 9.39 (תיאור שקול): נדרוש:

1. אם $i \neq j$ אז $|x_i - x_j| = 1$
2. לכל $x \in R$ קיים $i \in I$ כך ש $|x - x_i| < 1$ (ואז i יחיד)

הערה 9.40 מניחים בד"כ ש$0 \in \{x_i\}_{i\in I}$ (וגם ש $1 \in \{x_i\}_{i\in I}$)

9.13 דוגמה

נסתכל על $\mathbb{Q}$ עם ההערכה $|\cdot|_p$ (כאשר p ראשוני), כלומר

$$\left|p^n \cdot \frac{a}{b}\right|_p = \frac{1}{p^n}$$

כאשר a, b זרים לp. ברור שהשלמים הם שברים $p^n \cdot \frac{a}{b}$ עם $n \geq 0$ וa, b זרים לp). האידאל הקמסימלי מורכב מ$p^n \cdot \frac{a}{b}$ כאשר $n \geq 1$ וa, b זרים לp).

טענה 9.41 קבוצת נציגים נתונה ע"י $\{0, 1, \ldots, p-1\}$

הוכחה: התנאי הראשון מיידי. נבדוק את התנאי השני: יהי $x = p^n \cdot \frac{a}{b}$ עם a, b זרים לp ו$n > 0$. אם $n \geq 1$ נקח נציג 0. לכן נשאר לטפל במקרה בו $x = \frac{a}{b}$ כאשר a, b זרים לp. יש שלמים $h, k \in \mathbb{Z}$ כך ש$kb + hp = 1$ ואז

$$\begin{aligned}
\left|k - \frac{1}{b}\right|_p &= \left|\frac{hp}{b}\right|_p \\
&= |h|_p \cdot \left|\frac{1}{b}\right|_p \cdot |p|_p \\
&= |p|_p = \frac{1}{p} < 1
\end{aligned}$$

מכאן

$$\begin{aligned}
|x - ka|_p &= \left|\frac{a}{b} - ka\right|_p \\
&= \underbrace{|a|_p}_{1} \cdot \left|\frac{1}{b} - k\right|_p < 1
\end{aligned}$$

לבסוף, ka הוא שלם וברור שיש $0 \leq m \leq p-1$ עם $m = ka \pmod p$. ואז $|ka - m| <$ 1 ולכן $|x - m| < 1$. ■

מסקנה 9.42 שדה השארית של $\mathbb{Q}$ ביחס ל$|\cdot|_p$ הוא איזומורפי ל$\mathbb{Z}/p\mathbb{Z}$:

$$\mathbb{Z} \hookrightarrow R \quad \xrightarrow{\bar{\cdot}} \quad \overline{\mathbb{Q}}$$

נסמן $\varphi : \mathbb{Z} \to \overline{\mathbb{Q}}$ את ההעתקה $x \mapsto \overline{x}$. אז φ הומומורפיזם של חוגים ו$p \in \mathrm{Ker}\varphi$ ו$\varphi(1) = 1$ (כלומר $1 \notin \mathrm{Ker}\varphi$) ולכן φ משרה איזומורפיזם

$$\mathbb{Z}/p\mathbb{Z} \quad \cong \quad \overline{\mathbb{Q}}$$

הערה 9.43 $\mathbb{Z}$ צפוף בשלמים של $\left\{\mathbb{Q}, |\cdot|_p\right\}$.

הוכחה: יהי $x = p^n \cdot \frac{a}{b}$ שלם של $\mathbb{Q}$ (ביחס ל$|\cdot|_p$) עם a, b זרים לp ו$n \geq 0$. יהי $j > 0$. קיימים h, k עם $kb + hp^j = 1$. אז

$$\left|k - \frac{1}{b}\right| \quad = \quad \left|p^j \cdot \frac{h}{b}\right| \leq \frac{1}{p^j}$$

ולכן

$$\Bigg|x - \underbrace{p^n a k}_{\in \mathbb{Z}}\Bigg| \quad = \quad |p^n a| \left|\frac{1}{b} - k\right| \leq \frac{1}{p^{n+j}}$$

קטן כרצוננו (ע"י בחירת j גדול). ■

9.14 חבורת הערכה

נסמן

$$\left|K^{\times}\right| \quad = \quad \left\{|x| \mid x \in K^{\times}\right\} \subseteq (0, \infty)$$

זאת חבורה הנקראת חבורת ההערכה.

הערה 9.44 (דוגמה): עבור $K = \mathbb{Q}$:

- ל$|\cdot|_\infty$ יש חבורת הערכה: הרציונליים חיתוך $(0, \infty)$ (כלומר $\mathbb{Q} \cap (0, \infty)$ ביחס לכפל)
- ל$|\cdot|_p$ יש חבורה הערכה: $\{p^s \mid s \in \mathbb{Z}\}$

9.15 הרחבות שדות וe וf

טענה 9.45 תהי K/F הרחבה סופית של שדות. תהי $|\cdot|$ הערכה על K ו$|\cdot|_F$ הצמצום שלה על F. אז:

- $|\cdot|$ לא ארכימדית $\iff$ $|\cdot|_F$ לא ארכימדית (ראינו)
- $|\cdot|$ לא טריוואלית $\iff$ $|\cdot|_F$ לא טריוואלית.

הוכחה: $\Longrightarrow$: מיידי.

$\Longleftarrow$: נניח כי $|\cdot|_F$ טריוואלית. אז חוג ההערכה של $|\cdot|$ סגור בשלמות ($|\cdot|$ לא ארכימדי, כי אחרת $\mathbb{Q} \subseteq K$ והצמצום של $|\cdot|_F$ על $\mathbb{Q}$ ארכימדי ולכן שקול ל$|\cdot|_\infty$ ־ סתירה לטריוואליות על $\mathbb{Q} \subseteq F$). חוג הערכה זה מכיל את F. אבל K שלם מעל F ולכן חוג ההערכה שווה לK $\Longleftarrow$ $|\cdot|$ טריוואלית. ■

כעת נניח כי $|\cdot|$ ולא ארכימדית.

יהי R חוג השלמים של $|\cdot|$. אז $R_F = R \cap F$ חוג השלמים של $|\cdot|_F$. יהי P האידאל המקסימלי של R:

$$P \quad = \quad \{x \mid |x| < 1\}$$

אז $P_F = P \cap F$ הוא האידאל המקסימלי של R_F. מכאן מקבלים שיכון

$$\overline{F} = R_F/P_F \quad \hookrightarrow \quad R_K/P_K = \overline{K}$$

נתייחס לשוויון הזה כהכלה.

הגדרה 9.46 (סימון): $f = \left[\overline{K} : \overline{F}\right]$

מתקיים $|F^\times| = |F^\times|_F \subseteq |K^\times|$.

הגדרה 9.47 (סימון): $e = (|K^\times| : |F^\times|)$ (כלומר e האינדקס של $|F^\times|$ ב$|K^\times|$)

טענה 9.48 בסימונים אלה, $ef \leq [K : F]$ ובפרט e, f סופיות.

לפני ההוכחה ־ למה:

למה 9.49 יהיו $a_1, \ldots, a_l \in R$ כך ש$\overline{a_1}, \ldots, \overline{a_l} \in \overline{K}$ בלתי תלויים לינארית מעל $\overline{F}$. אז לכל $\gamma_1, \ldots, \gamma_l \in F$ לא כולם אפסים מתקיים

$$\left|\sum_{j=1}^{l} \gamma_j a_j\right| \quad = \quad \max_{1 \leq j \leq l} |\gamma_j| \in \left|F^\times\right|$$

הוכחה: אפשר להניח כי $\gamma_j \neq 0$ לכל j וש

$$|\gamma_1| \geq |\gamma_2| \geq \quad \ldots \quad \geq |\gamma_l| \geq 0$$

נסמן

$$b \quad = \quad a_1 + \frac{\gamma_2}{\gamma_1} a_2 + \cdots + \frac{\gamma_l}{\gamma_1} a_l \in R$$

כי $\frac{\gamma_i}{\gamma_1} \in R \cap F = R_F$ לכל $2 \leq i \leq l$. מתקיים

$$\overline{a_1} + \overline{\left(\frac{\gamma_2}{\gamma_1}\right)} \overline{a_2} + \cdots + \overline{\left(\frac{\gamma_l}{\gamma_1}\right)} \overline{a_l} \quad \neq \quad 0_{\overline{K}}$$

לאור האי־תלות ולכן $b \notin P_K$ ומכאן $|b| = 1$ ואז

$$\left|\sum_{j=1}^{l} \gamma_j a_j\right| = |\gamma_1| |b| = |\gamma_1| = \max_{1\le j\le l} |\gamma_j| \in \left|F^\times\right|$$

■

נעבור להוכחת הטענה. **הוכחה:** די להוכיח שאם $x_1, \ldots, x_k \in K^\times$ מקיימים שהקוסטים

$$|x_1| \left|F^\times\right|, \quad \ldots, \quad |x_k| \left|F^\times\right|$$

שונים זה מזה ושאם $a_1, \ldots, a_l \in R$ מקיימים ש־$\overline{a_1}, \ldots, \overline{a_l} \in \overline{K}$ בלתי תלויים לינארית מעל $\overline{F}$, אז $\{x_j \cdot a_j \mid i = 1, \ldots, k \mid j = 1, \ldots, l\}$ בלתי תלויים מעל F.

נוכיח בדרך השלילה: נניח שקיימים $c_{ij} \in F$ לא כולם אפסים כך ש־$\sum_{i,j} c_{ij} x_i a_j = 0$. אפשר להניח שלכל i קיים j כך ש־$c_{ij} \neq 0$ (אחרת נזרוק את x_i). נסמן $\lambda_i = \sum_j c_{ij} a_j$. אז לפי הלמה $|\lambda_i| \in |F^\times|$ (ובפרט $\lambda_i \neq 0$). לבסוף מתקיים $\sum_{i=1}^k \lambda_i x_i = 0$ עם $\lambda_i x_i \neq 0$ לכל i. לכן $k \geq 2$ וקיימים $i_1 \neq i_2$ עם $|\lambda_{i_1} x_{i_1}| = |\lambda_{i_2} x_{i_2}|$ ומכאן $|x_{i_1}| |F^\times| = |x_{i_2}| |F^\times|$. סתירה. ■

10 הערכות דיסקרטיות וחוגי דדקינד

הגדרה 10.1 הערכה נקראת דיסקרטית אם חבורת ההערכה שלה ציקלית (ולא טריוואלית).

הערה 10.2

1. כלומר אם קיים $0 < \gamma \neq 1$ כך ש $|K^\times| = \{\gamma^n \mid n \in \mathbb{Z}\}$. ($\gamma \neq 1$ כי $|\cdot|$ לא טריוואלית). בהמשך נניח כי $0 < \gamma < 1$ ואז γ יקבע ביחידות.

2. תנאי דיסקרטיות אינווריאנטי ביחס לשקילות.

3. $|\cdot|$ דיסקרטית $\Longleftarrow$ $|\cdot|$ לא ארכימדית.

   הוכחה: אם $\{K, |\cdot|\}$ ארכימדית אז $\mathrm{char} K = 0$ ולכן $\mathbb{Q} \subseteq K$ והצמצום על $\mathbb{Q}$ הוא מהצורה $|\cdot|_\infty^\rho$ - סתירה. ■

4. נסמן כרגיל $R = \{x \mid |x| \leq 1\}$ חוג ההערכה, $U = \{x \mid |x| = 1\}$ ההפיכים, $P = \{x \mid |x| < 1\}$ האידאל המקסימלי.

הגדרה 10.3 איבר $\pi \in K$ נקרא ראשוני אם $|\pi| = \gamma$. אז $\pi \in R$. אוסף הראשוניים הוא πU. $|\pi|$ נקבע באופן יחיד ע"י

1. $|\pi|$ יוצר את $|K^\times|$

2. $|\pi| < 1$

הערה 10.4 $|\pi|$ נקבע באופן יחיד גם ע"י $\{|\pi| = \max\{|x| \mid 0 < |x| < 1 \mid x \in K\}$. ל$x \in K^{\times}$ מתקיים $|x| = \gamma^n$. מסמנים $n = \mathrm{ord}_K(x)$ ־ הסדר של x. מתקיים

$$\begin{aligned} R &= \left\{x \in K^{\times} \mid \mathrm{ord}_K(x) \geq 0\right\} \cup \{0\} \\ U &= \left\{x \in K^{\times} \mid \mathrm{ord}_K(x) = 0\right\} \\ P &= \left\{x \in K^{\times} \mid \mathrm{ord}_K(x) > 0\right\} \cup \{0\} \\ &= \left\{x \in K^{\times} \mid \mathrm{ord}_K(x) \geq 1\right\} \cup \{0\} \end{aligned}$$

טענה 10.5 (כפליות): $\mathrm{ord}(xy) = \mathrm{ord}(x) + \mathrm{ord}(y)$ (ל$x, y \in K^{\times}$)

טענה 10.6 (פירוק איבר): לכל $x \in K^{\times}$ וπ ראשוני קיימים $n \in \mathbb{Z}$ ו$u \in U$ יחידים כך ש$x = \pi^n u$ ומתקיים

$$\begin{aligned} u &= \frac{x}{\pi^{\mathrm{ord}_K(x)}} \\ n &= \mathrm{ord}_K x \end{aligned}$$

הוכחה: קיום: ברור כי האיברים בטענה מקיימים את הדרוש. יחידות: אם $x = \pi^n u$ אז $|x| = |\pi^n u| = |\pi|^n$ ולכן $n = \mathrm{ord}_K x$) ■

הערה 10.7 n לא תלוי בבחירת π, u תלוי בבחירת π.

טענה 10.8 (פירוק $K^{\times}$): בהנתן π ראשוני יש איזומורפיזם של חבורות טופולוגיות

$$\begin{aligned} K^{\times} &\cong \mathbb{Z} \times U \\ x &\mapsto \left(\mathrm{ord}_K x, \frac{x}{\pi^{\mathrm{ord}_K x}}\right) \\ \pi^n u &\leftarrow (n, u) \end{aligned}$$

הוכחה: צריך לבדוק ש$\mapsto$ רציפה. די לבדוק כי $\mathrm{ord}_K(\cdot) : K^{\times} \to \mathbb{Z}$ רציפה. $\mathrm{ord}_K(\cdot)$ הומומורפיזם של חבורות. צריך רק לבדוק ש$\mathrm{Ker}\mathrm{ord}_K(\cdot) = U$ פתוחה וזה נכון. (כי אם $|\alpha| = 1$ ו$|\beta| < 1$ אז $|\alpha + \beta| = 1$) ■

הגדרה 10.9 (סימון): $P^n = \pi^n R = \{x \in K \mid |x| \leq |\pi|^n\}$ כאשר $n \in \mathbb{Z}$. אז P^n הוא תת־מודול של K, P^n תת חבורה פתוחה של $\langle K, +\rangle$ (ולכן גם סגורה) ומתקיים:

$$\cdots \supsetneqq P^{-1} \supsetneqq P^0 = R \supsetneqq P^1 = P \supsetneqq P^2 \quad \supsetneqq \quad \ldots$$

הערה 10.10 האידאלים (השלמים) השונים מאפס של R הם P^n כאשר $n \geq 0$.

הוכחה: יהי $0 \neq I \subseteq R$. נסמן $0 \leq n = \min\{\mathrm{ord}_K x \mid 0 \neq x \in I\}$ ואז יש $0 \neq x =$ $\pi^n u \in I$ ולכן $P^n = \pi^n R \subseteq I$. מצד שני לכל $0 \neq y \in I$ יש תיאור $y = \pi^{\mathrm{ord}_K y} \cdot u'$ (כאשר $u' \in U$) ומתקיים $\mathrm{ord}_K y \geq n$ ולכן $y \in P^n$. ■

מסקנה 10.11 כל אידאל שברי הינו מהסוג P^n.

הוכחה: אכן, הוא שלם כפול x עם פירוק $x = \pi^n u$. ■

טענה 10.12 R הוא חוג ראשי.

הערה 10.13

1. $x \in P^k \iff \mathrm{ord}_K x \geq k$ (כאשר $k \in \mathbb{Z}$ ו-$x \in K^\times$).

   הוכחה: $\Longrightarrow$: $x = x^{\mathrm{ord}_K x} u \in P^{\mathrm{ord}_K x} \subseteq P^k$

   $\Longleftarrow$: יש $y \in R$ עם $x = \pi^k y$. יש פירוק $y = \pi^{\mathrm{ord}_K y} \cdot u'$ עם $\mathrm{ord}_K y \geq 0$ ו-$u' \in U$ ולכן $x = \pi^{k+\mathrm{ord}_K y} u'$ ומכאן $\mathrm{ord}_K x = k + \mathrm{ord}_K y \geq k$. ■

2. $\mathrm{ord}_K x = \max\left\{k \mid x \in P^k\right\}$

3. הפונקציה $\mathrm{ord}_K : K^\times \to \mathbb{Z}$ אינווריאנטית לשקילות הערכתית (כי האיברים הראשוניים נשמרים).

10.1 הערכה מעריכית

הגדרה 10.14 יהי K שדה. פונקציה <u>על</u> $\nu : K^\times \to \mathbb{Z}$ נקראת הערכה מעריכית אם

1. $\nu(xy) = \nu(x) + \nu(y)$ לכל $x, y \in K^\times$

2. $\nu(x+y) \geq \min(\nu(x), \nu(y))$ (לכל $x, y, x+y \in K^\times$)

הערה 10.15 מסמנים $\nu(0) = \infty$ ואז התנאים בהגדרה נכונים לכל $x, y \in K$.

הערה 10.16 (דוגמה): תהי $|\cdot|$ הערכה דיסקרטית על K. אז $\mathrm{ord}_K \pi = 1$ ולכן ord_K על. התנאי $\mathrm{ord}_K(x) + \mathrm{ord}_K(y) = \mathrm{ord}_K(xy)$ מיידי. נבדוק את התנאי השני.
נסמן $k = \min(\mathrm{ord}_K x, \mathrm{ord}_K y)$. אז

$$\begin{aligned} x &\in P^{\mathrm{ord}_K x} \subseteq P^k \\ y &\in P^{\mathrm{ord}_K y} \subseteq P^k \end{aligned}$$

ולכן $x + y \in P^k$ ומכאן $\mathrm{ord}_K(x+y) \geq k = \min(\mathrm{ord}_K x, \mathrm{ord}_K y)$.

10.1.1 בניית הערכה דיסקרטית בעזרת הערכה מעריכית

תהי ν הערכה מעריכית של K. נבחר $0 < \gamma < 1$. נגדיר הערכה על K לפי $|0| = 0$ ו$|x| = \gamma^{\nu(x)}$. אז $|\cdot|$ הערכה דיסקרטית. אכן, די לבדוק את אי־שוויון המשולש הלא ארכימדי:

$$\begin{aligned} |x+y| = \gamma^{\nu(x+y)} &\leq \gamma^{\min(\nu(x),\nu(y))} \\ &= \max\left(\gamma^{\nu(x)}, \gamma^{\nu(y)}\right) \\ &= \max(|x|, |y|) \end{aligned}$$

הערה 10.17 מחלקת השקילות אינה תלויה בבחירת $0 < \gamma < 1$.

הערה 10.18 π ראשוני $\iff$ $\nu(\pi) = 1$.

מסקנה 10.19 קיימת התאמה חד־חד־ערכית ועל

$$\{\text{Exponential valuations on } K\} \quad \leftrightarrow \quad \{\text{Equivalence classes of discrete valuations on } K\}$$

ומתקיים:

$$\begin{aligned} R &= \{x \mid \nu(x) \geq 0\} = \{x \mid |x| \leq 1\} \\ P &= \{x \mid \nu(x) > 0\} = \{x \mid |x| < 1\} \\ U &= \{x \mid \nu(x) = 0\} = \{x \mid |x| = 1\} \end{aligned}$$

10.2 הערכות דיסקרטיות וDVR

תהי $|\cdot|$ הערכה דיסקרטית על K. אז חוג ההערכה

$$R = \{x \mid |x| \leq 1\}$$

הוא DVR וK שדה המנות של R. **הוכחה:** ראינו שR חוג ראשי , ובפרט חוג דדקינד, ויש לו אידאל מקסימלי יחיד

$$P = \{x \mid |x| < 1\}$$

(כי כזכור $R \setminus P$ הם ההפיכים). ■

בהנתן שדה K, יהי $K \subseteq R$ חוג DVR כך שK הינו שדה המנות של R. יהי $P \subseteq R$ האידאל המקסימלי היחיד. יהי $\pi \in P \setminus P^2$ ראינו (בפרק על DVR) שלכל $x \in K^\times$ יש פירוק יחיד $x = \pi^n u$ (באשר $n \in \mathbb{Z}$ ו$u \in U = R^\times$). נגדיר פונקציה

$$\begin{aligned} n : K^\times &\longrightarrow \mathbb{Z} \\ x &\mapsto n(x) := n \end{aligned}$$

(של הפירוק לעיל). אז n הערכה מעריכית על K. **הוכחה:** אכן, ברור שn על וכפלית. צריך לבדוק שאכן

$$n\left(x+y\right) \quad \geq \quad \min\left(n\left(x\right),n\left(y\right)\right)$$

אם $k\leq n\left(x\right)$ אז $x\in\pi^{n(x)}R\subseteq\pi^{k}R$ ובאופן דומה אם $k\leq n\left(y\right)$ אז $y\in\pi^{n(y)}R$. לכן ל$k=\min\left(n\left(x\right),n\left(y\right)\right)$, מתקיים כי $x,y\in\pi^{k}R$ ולכן $x+y\in\pi^{k}R$ ולכן יש $r\in R$ עם $x+y=\pi^{k}r$. אם $x+y\neq0$ אז יש פירוק $r=\pi^{n(r)}u'$ (כאשר $u'\in U$ ו$n\left(r\right)\geq0$) ולכן

$$x+y \quad = \quad \pi^{k+n(r)}u'$$

ומכאן $n\left(x+y\right)=k+n\left(r\right)\geq k$. ■

מסקנה 10.20 יש התאמות חד־חד־ערכיות ועל

$$\begin{array}{ccc}\{\text{DVR in } K \text{ which their field of fractions is } K\} & \leftrightarrow & \{\text{Equivalence classes of discrete valuations on } K\}\\ \updownarrow & \nearrow & \\ \{\text{Exponential valuations on } K\} & & \end{array}$$

טענה 10.21 (איפיון): יהי R חוג DVR, K שדה המנות ו$n:K^{\times}\to\mathbb{Z}$ ההערכה המתאימה. תהי $\left|\cdot\right|:K\to\left[0,\infty\right)$ הערכה לא ארכימדית ולא טריוואלית, ונסמן ב

$$R_{\left|\cdot\right|} \quad = \quad \left\{x\in K\mid\left|x\right|\leq1\right\}$$

את חוג ההערכה שלה. אם $R\subseteq R_{\left|\cdot\right|}$ אז $R=R_{\left|\cdot\right|}$ ו$\left|\cdot\right|$ דיסקרטית ומתאימה לn.

הוכחה: $R_{\left|\cdot\right|}\neq K$ (כי $\left|\cdot\right|$ לא טריוואלית). מתוך $R\subseteq R_{\left|\cdot\right|}\subsetneqq K$ וממקסימליות R נובע כי $R=R_{\left|\cdot\right|}$.

לכל $u\in U=R^{\times}$ מתקיים $\left|u\right|=1$: אכן $u^{\pm1}\in R=R_{\left|\cdot\right|}$ ולכן $\left|u\right|=1$. יהי P האידאל המקסימלי של R ו$\pi\in P\setminus P^{2}$. יהי $x\in K^{\times}$. מהפירוק $x=\pi^{n(x)}\cdot u$ עם $u\in U$ נקבל

$$\left|x\right| \quad = \quad \left|\pi\right|^{n(x)}\left|u\right|=\left|\pi\right|^{n(x)}$$

ולכן $\left|K^{\times}\right|=\left\{\left|\pi\right|^{n}\mid n\in\mathbb{Z}\right\}$ ולכן $\left|\cdot\right|$ דיסקרטית ו$\gamma=\left|\pi\right|$ יוצר של $\left|K^{\times}\right|$ ב$\left(0,1\right)$. לבסוף, השוויון $\left|x\right|=\left|\pi\right|^{n(x)}$ מראה שההערכה המעריכית של $\left|\cdot\right|$ היא n. ■

10.3 הערכות על חוגי דדקינד

תזכורת: יהי R חוג דדקינד. K שדה המנות. נסמן בΣ את אוסף האידאלים הראשוניים השונים מאפס, ו$\mathfrak{F}\left(R\right)$ את אוסף האידאלים השבריים. ראינו שקיימות פונקציות יחידות

$$\begin{array}{rl}\left(P\in\Sigma\right) & \nu_{P}:\mathfrak{F}\left(R\right)\to\mathbb{Z}\\ \left(I\in\mathfrak{F}\left(R\right)\right) & I=\prod_{P\in\Sigma}P^{\nu_{P}(I)}\end{array}$$

ולכל $I\in\mathfrak{F}\left(R\right)$ מתקיים $\nu_{P}\left(I\right)=0$ כמעט לכל P ו$I\subseteq R\iff\nu_{P}\left(I\right)\geq0$ (לכל $P\in\Sigma$).

הערה 10.22 יהי $\langle R, P\rangle$ חוג DVR עם שדה מנות K. אז הפונקציה n המתאימה לו מקיימת $n\left(x\right)=\nu_{P}\left(xR\right)$ ($x\in K^{\times}$), ובפרט צד ימין מתאר הערכה מעריכית של K (כי צד שמאל כזה).

הוכחה:

$$\begin{aligned} P^{\nu_{P}(xR)} & = xR\\ & = \left(\pi^{n(x)}\underbrace{u}_{\in U}\right)R\\ & = \pi^{n(x)}R\\ & = P^{n(x)}\end{aligned}$$

■

מסקנה 10.23 יהי R חוג דדקינד עם שדה מנות K. אז לכל אידאל ראשוני $0\neq P\subseteq R$ הפונקציה $\nu_{P}:\mathfrak{F}\left(R\right)\rightarrow\mathbb{Z}$ מגדירה הערכה מעריכית לפי

$$\begin{aligned} K^{x} & \longrightarrow \mathbb{Z}\\ x & \mapsto \nu_{P}\left(xR\right)\end{aligned}$$

הוכחה: הפונקציות ν_{P} מתנהגות יפה במיקום

$$\nu_{P}^{R}\left(xR\right) = \nu_{P\cdot R_{P}}^{R_{P}}\left(xR_{P}\right)$$

ולאור ההערה הקודמת, צד ימין הינו הערכה מעריכית על K. ■

הגדרה 10.24 (סימון): נסמן את ההערכה המעריכית המתקבלת באותו שם:

$$\nu_{P}\left(x\right)=\nu_{P}\left(xR\right)\qquad\left(x\in R\right)$$

ו־$\nu_{P}\left(0\right)=\infty$. לכל $0<\gamma_{P}<1$ נקבל הערכה $\left|\cdot\right|_{P}$ מתאימה ל־P, ν_{P} ע"י

$$\begin{aligned} \left|x\right|_{P} & = \gamma_{P}^{\nu_{P}(x)}=\gamma_{P}^{\nu_{P}(xR)}\\ \left|0\right| & = 0\end{aligned}$$

הערה 10.25 $x\in R\iff\left|x\right|_{P}\leq1$ (כי $\nu_{P}\left(xR\right)\geq0$).

הגדרה 10.26 (מינוח, לא סטנדרטי): יהי R חוג דדקינד ו־$\left|\cdot\right|$ הערכה לא ארכימדית על שדה המנות K. נאמר ש־$\left|\cdot\right|$ הערכה <u>על R</u> אם $\left|x\right|\leq1$ (לכל $x\in R$), כלומר אם $R\subseteq R_{\left|\cdot\right|}$.

מסקנה 10.27 ν_{P} הערכה על R לכל $0\neq P\subseteq R$ ראשוני.

הערה 10.28 $x \in P \iff |x|_P < 1$

הוכחה: $xR \subseteq P$ ולכן $\nu_P(xP) \geq \nu_P(P) = 1$ ואז $|x|_P = \gamma_P^{\nu_P(x)} \leq \gamma_p < 1$ ■

הערה 10.29 חוג ההערכה של $|\cdot|_P$ הוא R_P והאידאל המקסימלי הוא PR_P.

הוכחה: יהי $z \in R_P$ אז $z = \frac{r}{s}$ כאשר $r \in R$ ו$s \in R \setminus P$. מההערות הקודמות מתקיים $|r|_P \leq 1$ ו$|s|_P = 1$ ולכן $|z|_P \leq 1$ ומכאן $z \in R_{|\cdot|_P}$. לכן $R_P \subseteq R_{|\cdot|_P}$ ומאחר ש$R_{|\cdot|_P} \neq K$ נובע ש $R_P = R_{|\cdot|_P}$.
ראינו שPR_P הוא האידאל המקסימלי היחיד של R_P וניתן לבדוק שאכן

$$PR_P \quad = \quad \{z \in K \mid |z|_P < 1\}$$

באותה צורה. ■

הערה 10.30 אם $a \in K^\times$ אז $\nu_P(a) = 0$ כמעט לכל P (כי $\nu_P(aR) = 0$ כמעט לכל P).

10.4 איפיון ν_P ו$|\cdot|_P$

טענה 10.31 יהי R חוג דדקינד, K שדה המנות, $0 \neq P \subseteq R$ ראשוני. תהי $|\cdot|$ הערכה לא ארכימדית ולא טריוואלית על K ויהי $R_{|\cdot|}$ חוג ההערכה של $|\cdot|$. אם $R_P \subseteq R_{|\cdot|}$ אז $R_P = R_{|\cdot|}$. בנוסף $|\cdot|$ דיסקרטית, ו$|\cdot|$ ו$|\cdot|_P$ שקולות (ובפרט $|\cdot|$ מתאימה להערכה המעריכית ν_P).

הוכחה: נובע מהעובדה שR_P הינו DVR וטענה מתאימה במקרה של DVR. ■

טענה 10.32 יהי R חוג דדקינד, K שדה המנות, Σ אוסף הראשוניים השונים מאפס של R.
לכל $P \in \Sigma$ נשתמש בסימון לעיל $\nu_P(x) = \nu_P(xR)$. תהי $|\cdot|_P$ הערכה מתאימה לP:

$$\begin{aligned} |x|_P &= \gamma_P^{\nu_P(x)} \qquad \left(x \in K^\times\right) \\ 0 &< \gamma_P < 1 \end{aligned}$$

1. ההערכות ν_P (ל$P \in \Sigma$) שונות זו מזו.
2. ההערכות $|\cdot|_P$ הן דיסקרטיות ולא שקולות זו לזו.
3. תהי $|\cdot|$ הערכה לא ארכימדית ולא טריוואלית על R (המינוח הלא סטנדרטי). אז קיים $P \in \Sigma$ יחיד כך ש$|x| < 1$ לכל $x \in P$ ובמקרה זה $|\cdot|$ היא שקולה ל$|\cdot|_P$ ובפרט $|\cdot|$ היא דיסקרטית.

הוכחה: ראינו ש$|\cdot|_P$ היא דיסקרטית. 1 נכון כי לכל $P, P' \in \Sigma$ עם $P \neq P'$ נקח $x \in P \setminus P'$ ואז $xR \not\subseteq P'$ ו $xR \subseteq P$ ולכן $\nu_P(xR) \geq 1$ ו$\nu_{P'}(xR) = 0$ ולכן $\nu_P(x) \neq \nu_{P'}(x)$. לכן 1 נכון ו2 נובע מ1.

נוכיח את 3: נתון $|x| \leq 1$ לכל $x \in R$. קיים $x \in R$ עם $|x| < 1$ (כי אחרת $|x| = 1$ לכל $0 \neq x \in R$ ואז $|\cdot|$ טריוואלית). נסמן

$$P = \{x \in K \mid |x| < 1\}$$

אז $0 \neq P \subsetneqq R$ ומתכונות ההערכה ומכך ש$|x| \leq 1$ לכל $x \in R$ נובע שP אידאל בR. כמו כן, P אידאל ראשוני כי אם $x, y \in R$ אז $|x|, |y| \leq 1$ ואם $xy \in P$ אז $|xy| < 1$ ולכן $|x| < 1$ או $|y| < 1$ כלומר $x \in P$ או $y \in P$.

לכל $s \in R \setminus P$ מתקיים $|s| = 1$.

יהי $z \in R_P$ אז $z = \frac{x}{s}$ עם $x \in R$ ו$s \in R \setminus P$ ולכן $|z| = \left|\frac{x}{s}\right| \leq 1$. מכאן נובע ש$R_P \subseteq R_{|\cdot|}$ וראינו שנובע ש$|\cdot|_P$ ו$|\cdot|$ שקולות. לאור 2 נובע גם שP עם התכונה $|x| < 1$ לכל $x \in P$ הוא יחיד. ■

10.5 משפט קירוב לחוגי דדקינד

(מבוסס על Weiss)

יהי R חוג דדקינד. יהי K שדה המנות. נסמן בΣ את אוסף הראשוניים השונים מאפס. לכל $P \in \Sigma$ נשתמש בν_P ו$|\cdot|_P$. אז $|\cdot|_P$ מגדירה טופולוגיה על K: כאן $x_n \longrightarrow 0$ אם $|x_n|_P \longrightarrow 0$ (או לחלופין אם $\nu_P(x_n) \longrightarrow \infty$)

משפט 10.33 תהי $S = \{P_1, \ldots, P_r\} \subseteq \Sigma$ (כאשר $P_1, \ldots, P_r$ שונים זה מזה). יהיו $a_1, \ldots, a_r \in K$ ו$m_1, \ldots, m_r$ טבעיים. אז קיים $a \in K$ כך ש

$$\begin{aligned} \nu_{P_i}(a - a_i) &\geq m_i \qquad (i = 1, \ldots, r) \\ \nu_P(a) &\geq 0 \qquad (P \in \Sigma \setminus S) \end{aligned}$$

הערה 10.34 אם $a_i \in R$ ו$m_i \geq 0$ (לכל i) אז נקבל $a \in R$ (כי $\nu_P(aR) = \nu_P(a) \geq 0$ לכל $P \in \Sigma$).

הוכחה: נזכור כי לכל $\alpha \in K$ מתקיים $\nu_P(\alpha) \geq 0$ כמעט לכל $P \in \Sigma$. לכן ניתן להגדיל את S באופן הבא: קיימים

$$P_{r+1}, \ldots, P_l \in \Sigma \setminus S$$

כך ש

$$\nu_P(a_i) \geq 0 \qquad \left(\substack{i=1,\ldots,r \\ P \notin \{P_1,\ldots,P_l\}}\right)$$

לכן ניתן להניח מראש שנתון $\nu_P(a_i) \geq 0$ לכל $P \in \Sigma \setminus S$. (נוסיף $a_i = 1$ עבור $i = r+1, \ldots, l$)

כעת יהי $j \in \{1, \ldots, r\}$. לכל k טבעי מתקיים

$$P_j^k + (P_1 \cdot \cdots \cdot P_{j-1} \cdot P_{j+1} \cdot \cdots \cdot P_r)^k = R$$

(מהמשפטים על ν_P בפרק על חוגי דדקינד) ולכן קיימים $x \in \left(P_1 \cdot \dots \cdot \widehat{P_j} \cdot \dots \cdot P_r\right)^k$ ו$y \in P_j^k$ עם $y + x = 1$ ואז

$$\begin{aligned} \nu_{P_j}(x-1) = \nu_{P_j}(y) & \\ \nu_{P_i}(x) \geq k & \qquad (i \neq j) \\ \nu_P(x) \geq 0 & \qquad (P \in \Sigma) \end{aligned}$$

נעבור לטופולוגיות. נסיק כי קיימת סדרה $\{x_{j,n}\}_{n=1}^{\infty}$ ל$j = 1, \dots, r$ כך ש $x_{j,n} \xrightarrow[n\to\infty]{} 1$ בטופולוגיה של $|\cdot|_j$, וכך ש$x_{j,n} \xrightarrow[n\to\infty]{} 0$ בטופולוגיה $|\cdot|_i$ ל$i \neq j$, ומתקיים $\nu_P(x_{j,n}) \geq 0$ (לכל j, n ו$P \in \Sigma$).

לבסוף נסמן $x_n = \sum_{j=1}^r x_{j,n} a_j$ ($n = 1, 2, \dots$) אז $x_n \xrightarrow[n\to\infty]{} a_j$ בטופולוגיה של $|\cdot|_j$ ולכל $P \in \Sigma \setminus S$ מתקיים

$$|x_n|_P \quad \leq \quad \max_{j=1}^{r} \left(|x_{j,n}|_p \cdot |a_j|_p\right) \leq 1$$

לבסוף ניתן לקחת $a = x_n$ עבור n גדול דיו. ■

מסקנה 10.35 באותם סימונים קיים $b \in K^\times$ כך ש$\nu_{P_i}(b) = m_i$ (עבור $i = 1, \dots, m$) ו$\nu_P(b) \geq 0$ (עבור $P \in \Sigma \setminus S$).

הערה 10.36 m_i נתונים מראש, ואם $m_i \geq 0$ אז $b \in R$.

הוכחה: לכל $i = 1, \dots, r$ נקח $a_i \in K$ עם $\nu_{P_i}(a_i) = m_i$ ונבחר $b \in K$ עם $\nu_P(b - a_i) \geq m_i + 1$ (לכל $i = 1, \dots, r$) ו$\nu_P(b) \geq 0$ (לכל $P \in \Sigma \setminus S$). אז

$$|b - a_i|_P \quad < \quad |a_i|_P$$

ולכן

$$|b_i|_{P_i} \quad = \quad |a_i|_P$$

כלומר $\nu_{P_i}(b) = \nu_{P_i}(a_i) = m_i$. בפרט $b \neq 0$. ■

הערה 10.37 אם $R = \mathbb{Z}$ אז המסקנה הזאת היא משפט השאריות הסיני.

מסקנה 10.38 יהי R חוג דדקינד. אם לR מספר סופי של אידאלים ראשוניים השונים מאפס אז R תחום ראשי.

הוכחה: במקרה זה נקבל מצב בו $\Sigma = \{P_1, \dots, P_r\}$. יהי $0 \neq I \subseteq R$ אידאל ו

$$I \quad = \quad P_1^{m_1} \cdot \dots \cdot P_r^{m_r}$$

הפירוק. יהי $a \in K^\times$ כמו במסקנה הקודמת (עם $\nu_{P_i}(b) = m_i$). אז

$$\nu_{P_i}(aR) = \nu_{P_i}(a) = m_i = \nu_{P_i}(I) \qquad (i = 1, \dots, r)$$

כלומר $\nu_P(aR) = \nu_P(I)$ (לכל $P \in \Sigma$), ומכאן $I = aR$. ■

מסקנה 10.39 כל אידאל בחוג דדקינד נוצר ע"י שני איברים.

הוכחה: בסימונים לעיל, יהי $I \subseteq R$ $0 \neq$ אידאל ו־$I = P_1^{m_1} \cdot \cdots \cdot P_r^{m_r}$ הפירוק. אז $m_i \geq 0$ ויש $a \in R$ עם $\nu_{P_i}(a) = m_i$ (ל־$i = 1, \ldots, r$) ו־$\nu_P(a) \geq 0$ (לכל $P \in \Sigma$). כלומר יש אידאלים ראשוניים $P_{r+1}, \ldots, P_l$ כך ש

$$aR = \left(P_1^{m_1} \cdot \cdots \cdot P_r^{m_r}\right)\left(P_{r+1}^{m_{r+1}} \cdot \cdots \cdot P_l^{m_l}\right)$$

עבור $m_{r+1}, \ldots, m_l \geq 0$ מתאימים. (כאן $P_1, \ldots, P_l$ שונים זה מזה)

יהי $b \in R$ כך ש־$\nu_{P_i}(b) = m_i$ (ל־$i = 1, \ldots r$) ו־$\nu_{P_i}(b) = 0$ (ל־$i = r+1, \ldots, l$) ו־$\nu_P(b) \geq 0$ (לכל $P \in \Sigma$). אז $b \in R$ והפירוק של bR הינו

$$bR = \left(P_1^{m_1} \cdot \cdots \cdot P_r^{m_r}\right)\left(P_{r+1}^{0} \cdot \cdots \cdot P_l^{0}\right)\left(P_{l+1}^{m_{l+1}} \cdot \cdots \cdot P_t^{m_t}\right)$$

מהפירוקים לעיל נובע כי $aR + bR = I$. ■

10.6 שדה שארית בהערכות מעל חוג דדקינד

יהי R חוג דדקינד, K שדה המנות, $0 \neq P \subseteq R$ ראשוני. תהי ν_P ההערכה המעריכית המתאימה ו־$|\cdot|_P$ ההערכה המתאימה ל־P. הגדרנו שדה שארית:

1. בשפה של חוגי דדקינד: R/P
2. בשפה של הערכות: R_P/PR_P

יש איזומורפיזם של חוגים

$$\begin{array}{ccc} R/P & \xrightarrow{\pi} & R_P/PR_P \\ r+P & \mapsto & r+PR_P \end{array}$$

אכן, פעולת כפל באיברי $S = R \backslash P$ על R/P הפיכה ולכן $R/P = (R/P)_P \cong R_P/PR_P$.

10.7 הרחבות ספרביליות

יהי $\mathcal{O}$ חוג דדקינד עם שדה מנות F, ותהי K/F הרחבה ספרבילית סופית, ו־R הסגור השלם של $\mathcal{O}$ ב־K. יהי $0 \neq P \subseteq \mathcal{O}$ ראשוני, ויהי $Q \subseteq R$ אידאל ראשוני מעל P (כלומר $Q \cap \mathcal{O} = P$). אז ישנן הערכות מעריכיות ν_P על F, ν_Q על K ולכל בחירה $0 < \gamma_Q, \gamma_P < 1$ נקבל הערכות על F ו־K ע"י $|x|_P = \gamma_P^{\nu_P(x)}$ ו־$|y|_Q = \gamma_Q^{\nu_Q(y)}$ (באשר $x \in F^\times$ ו־$y \in K^\times$). כמו כן, במסגרת חוגי דדקינד הגדרנו מספרים e_Q שהוא המעריך של Q בפירוק $PR = Q^{e_Q} \cdot \ldots$ ו־$f_Q = f = [R/Q : \mathcal{O}/P]$.

טענה 10.40 בסימונים אלה אם נבחר $\gamma_P = \gamma_Q^{e_Q}$ אז $|\cdot|_Q$ הרחבה של $|\cdot|_P$ על K. כמו כן, המספרים e ו־f מתורת ההערכות שווים למספרים e ו־f מחוגי דדקינד המתוארים לעיל.

הערה 10.41 נראה שהתנאי $\gamma_P = \gamma_Q^{e_Q}$ הכרחי.

הוכחה: לכל $x \in F$ יש פירוק $x\mathcal{O} = P^{\nu_P(x)} \cdot \ldots$ ולכן $R = (x\mathcal{O})\,R = Q^{e_Q \nu_P(x)} \cdot \ldots$ (כי

$$\begin{aligned} x\mathcal{O}R &= P^{\nu_P(x)} \cdot \ldots \cdot R \\ &= (PR)^{\nu_P(x)} \cdot \ldots \\ &= \left(Q^{e_Q} \cdot \ldots\right)^{\nu_P(x)} \cdot \ldots \end{aligned}$$

)

מכאן $|x|_P = \gamma_P^{\nu_P(x)}$ ו-$|x|_Q = \gamma_Q^{e_Q \cdot \nu_P(x)}$. לכן $|\cdot|_Q$ הרחבה של $|\cdot|_P$ אם ורק אם מתקיים $\gamma_P = \gamma_Q^{e_Q}$. כמו כן $|F^\times|_P = \{\gamma_P^n\}_{n=-\infty}^{\infty} = \left\{\gamma_Q^{e_Q \cdot n}\right\}_{n=-\infty}^{\infty}$ ו-$|K^\times|_Q = \left\{\gamma_Q^n\right\}_{n=-\infty}^{\infty}$. לכן $e_Q = (|K^\times| : |F^\times|)$.

לגבי שוויון ה-fים: בשני המקרים f מוגדר כדרגת הרחבת שדה השארית וראינו ששדות השארית זהים קנונית. ■

טענה 10.42 באותם סימונים, תהי $|\cdot|'$ הערכה על K המחזירה את $|\cdot|_P$ על F. אז קיים אידאל ראשוני (יחיד) $0 \neq Q \subseteq K$ כך ש-$|\cdot|'$ מתאימה ל-Q, ובמקרה זה Q הוא מעל P.

הוכחה: $|\cdot|_P$ לא ארכימדית $\Longleftarrow$ $|\cdot|'$ לא ארכימדית. $\mathcal{O}$ מוכל בחוג השלמים של $|\cdot|_P$ ולכן של $|\cdot|'$, אבל חוג השלמים של $|\cdot|'$ סגור בשלמות, ולכן R מוכל בחוג השלמים של $|\cdot|'$. כלומר $|\cdot|'$ הערכה על R. במצב זה ראינו קיום Q וגם יחידות. לבסוף

$$\begin{aligned} \mathcal{O} \cap Q &= \mathcal{O} \cap \left\{ y \in K \mid |y|' < 1 \right\} \\ &= \left\{ x \in \mathcal{O} \mid |x|_P < 1 \right\} \\ &= P \end{aligned}$$

ולכן Q מעל P. ■

מסקנה 10.43 בסימונים לעיל יהי $PR = Q_1^{e_1} \cdot \ldots \cdot Q_r^{e_r}$ הפירוק (עם $Q_i \neq Q_j$ ל-$i \neq j$ ו-$e_i \geq 1$ לכל i) אז ל-$|\cdot|_P$ על F יש בדיוק r הרחבות לא שקולות להערכות על K והן מתאימות לאידאלים $Q_1, \ldots, Q_r$ ומספרי e הם $e_1, \ldots, e_r$ ומספרי f שלהם הם מספרי f הרגילים $[R/Q_i : \mathcal{O}/P]$.

10.7.1 יישום להערכות דיסקרטיות

טענה 10.44 תהי K/F הרחבה ספרבילית סופית של שדות ותהי $|\cdot|$ הערכה דיסקרטית על F. אז קיימת הרחבה של $|\cdot|$ להערכה על K, ומספר ההרחבות האלה סופי וכולן דיסקרטיות ואינן שקולות זו לזו. נסמן הרחבות אלו ב-$|\cdot|_1, \ldots, |\cdot|_r$. אז מתקיים

$$\sum_{i=1}^{r} e_i f_i = [K : F]$$

כאשר $f_i = \left[\overline{K} : \overline{F}\right]$ (כאשר $\overline{K}, \overline{F}$ שדות השארית לפי $|\cdot|_i$) ו-$e_i = (|K^\times|, |F^\times|)$.

הוכחה: נסמן $\mathcal{O} = \{x \in F \mid |x| \leq 1\}$. אז $\mathcal{O}$ הוא DVR ובפרט חוג דדקינד עם שדה מנות F. הטענה נובעת מטענות קודמות: יש לשים לב שאם $|\cdot|_i \neq |\cdot|_j$ נובע ש-$|\cdot|_i$, $|\cdot|_j$ אינן שקולות (כי שתיהן מרחיבות את $|\cdot|$ על F שאינה טריוואלית). ■

<u>עד כאן אלגברה ללא גבולות.</u>

11 הערכות שלמות

הגדרה 11.1 הערכה $|\cdot|$ של שדה F נקראת שלמה אם לכל סדרה $x_n \in F$ ($n = 1, 2, \ldots$) כך ש$\lim_{m,n\to\infty} |x_n - x_m| = 0$ קיים גבול $\lim_{n\to\infty} x_n = x \in F$ (כלומר $\lim_{n\to\infty} |x_n - x| = 0$).

הערה 11.2 תנאי זה אינווריאנטי לשקילות הערכות.

אם $|\cdot|$ ערך מוחלט, אז ראינו ש$d(x, y) = |x - y|$ מגדירה מטריקה ואז הדרישה היא שF שלם כמרחב מטרי.

11.1 מרחבים נורמיים

הגדרה 11.3 הגדרה יהי $\langle F, |\cdot| \rangle$ שדה הערכה. מרחב נורמי $\langle V, |\cdot| \rangle$ מעל $\langle F, |\cdot| \rangle$ הוא מרחב וקטורי V מעל F ופונקציה $|\cdot| : V \to [0, \infty)$ כך ש:

1. $|v| = 0 \iff v = 0$
2. $|\lambda v| = |\lambda| \cdot |v|$
3. $|u + v| \le |u| + |v|$

(לכל $u, v \in V$ ו$\lambda \in F$)

הערה 11.4 אם $V \neq 0$ נובע ש$|\cdot|$ ערך מוחלט על F.

הוכחה: נקח $0 \neq v \in V$ ולכל $\alpha, \beta \in F$ מתקיים

$$\begin{aligned} |\alpha + \beta| \, |v| &= |(\alpha + \beta) v| \\ &= |\alpha v + \beta v| \\ &\le |\alpha v| + |\beta v| \\ &= (|\alpha| + |\beta|) \, |v| \end{aligned}$$

ולכן $|\alpha + \beta| \le |\alpha| + |\beta|$. ■

הגדרה 11.5 שתי נורמות $|\cdot|_1$ ו$|\cdot|_2$ על V נקראות שקולות אם קיימים $c_1, c_2 > 0$ כך ש

$$c_2 |v|_2 \quad \le \quad |v|_1 \le c_1 |v|_2$$

הערה 11.6 נורמה מגדירה מטריקה ושתי נורמות שקולות מגדירות אותה טופולוגיה.

הערה 11.7 (דוגמה): אם $\dim_F V = n < \infty$ ואם $\mathcal{B} = \{v_1, \ldots, v_n\}$ בסיס של V מעל F, יש נורמות

$$\begin{aligned} \left| \sum_{i=1}^{n} \lambda_i v_i \right|_1 &= \sum_{i=1}^{n} |\lambda_i| \\ \left| \sum_{i=1}^{n} \lambda_i v_i \right|_\infty &= \max_{i=1}^{n} |\lambda_i| \end{aligned}$$

והן שקולות.

הערה 11.8 אם F שלם אז V מרחב שלם ביחס לכל אחת מנורמות אלה.

משפט 11.9 יהי F שדה עם הערכה שלמה $|\cdot|$. יהי V מרחב וקטורי מעל F בעל מימד סופי. אז

1. כל הנורמות של V מעל $\langle F,|\cdot|\rangle$ שקולות.
2. V מרחב שלם ביחס לכל נורמה מעליו.
3. אם W מרחב נורמי מעל F אז כל תת־מרחב $U\subseteq W$ בעל מימד סופי הוא סגור.

הוכחה: ברור ש־$1 \Longleftarrow 2,3$.
נוכיח את הטענה באינדוקציה על $n=\dim_F V$. עבור $n=0$ זה ברור.
יהי V מרחב נורמי ממימד $n+1$. יהי $\mathcal{B}=\{v_0,\ldots,v_n\}$ בסיס. ממנו נקבל $|\cdot|_\infty$. נראה ש־$|\cdot|$ שקולה ל־$|\cdot|_\infty$. ראשית:

$$\begin{aligned}\left|\sum_{i=0}^n\lambda_iv_i\right| &\leq \sum_{i=0}^n|\lambda_i|\,|v_i|\\ &\leq \max_{i=0}^n|\lambda_i|\cdot\sum_{i=0}^n|v_i|\\ &= \underbrace{\sum_{i=0}^n|v_i|}_{C}\cdot\left|\sum_{i=0}^n\lambda_iv_i\right|_\infty\end{aligned}$$

צריך להוכיח את האי־שוויון ההפוך. לכל $i=0,\ldots,n$ נסמן תת־מרחב

$$V_i = \operatorname{span}_F\{v_0,\ldots,v_{i-1},v_{i+1},\ldots,v_n\}$$

אז $V_i\subseteq V$ סגור ב־V. לכן הקבוצה

$$P = \bigcup_{i=0}^n(v_i+V_i)$$

סגורה ב־V וברור ש־$0\notin P$.
לכן קיים $\rho>0$ כך ש־$B(0,\rho)\cap P=\emptyset$, כאשר

$$B(0,\rho) = \{v \mid |v|<\rho\}$$

נראה של־$v\in V$ מתקיים $|v|<\rho \Longleftarrow |v|_\infty<1$. אכן יהי $v=\sum_{i=0}^n\mu_iv_i$ עם $|v|<\rho$.
די להראות $|\mu_i|<1$ לכל i.
נראה זאת בדרך השלילה: נניח כי $|\mu_{i_0}|=\max|\mu_i|\geq 1$ אז $\mu_{i_0}^{-1}v\in B(0,\rho)$ (כי $\left|\mu_{i_0}^{-1}v\right|=|\mu_{i_0}|^{-1}|v|<\rho$).
מצד שני $\mu_{i_0}^{-1}v\in v_{i_0}+V_{i_0}$. סתירה.

לבסוף יהי $a\in F^{\times}$ עם $|a|<1$. לכל $0\neq u\in V$ קיים $n\in\mathbb{Z}$ כך ש

$$|a|^2\rho<|a^nu| \quad = \quad |a|^n|u|<\rho$$

(כי $\Longleftrightarrow$

$$\frac{\rho}{|u|}|a|^2 \quad < \quad |a|^n<\frac{\rho}{|u|}$$

ויש מספר שלם בקטע $\left[\log_{|a|}\left(\frac{\rho}{|u|}\right)-2,\log_{|a|}\left(\frac{\rho}{|u|}\right)\right]$ כי זהו קטע באורך גדול מ1)
ולכן $|a^nu|_\infty<1$ ומכאן

$$|u|_\infty<|a|^{-n} \quad < \quad \frac{|a|^{-2}}{\rho}|u|$$

ולכן $|\cdot|$ שקול ל$|\cdot|_\infty$ ו1 נכון לV. ■

11.2 הרחבות סופיות ספרביליות

משפט 11.10 יהי $\langle F,|\cdot|\rangle$ שדה הערכה שלם לא טריוואלי ונניח ש$\langle F,|\cdot|\rangle$ ארכימדי או דיסקרטי. תהי K/F הרחבה ספרבילית סופית של שדות ונסמן $n=[K:F]$. אז קיימת הרחבה אחת ויחידה $|\cdot|_K$ של $|\cdot|$ על K והיא נתונה ע"י

$$|x|_K=\sqrt[n]{N_{K/F}(x)} \qquad (x\in K)$$

ו$\langle K,|\cdot|_K\rangle$ שלם.

הוכחה: ע"י החלפת $|\cdot|$ ב$|\cdot|^\rho$ $(\rho>0)$ אפשר להניח כי $|2|\leq 2$ ואז $|\cdot|$ ערך מוחלט.
יחידות: כל הרחבה $|\cdot|_K$ של $|\cdot|$ היא ערך מוחלט ולכן הופכת את $\langle K,|\cdot|_K\rangle$ למרחב נורמי מעל $\langle F,|\cdot|_F\rangle$. מכאן נובע שכל שתי הרחבות של ההערכה לK הן שקולות במובן של מרחבים נורמיים (כלומר $c_2|\cdot|_K'\leq|\cdot|_K\leq c_1|\cdot|_K'$). לכן הן יוצרות אותה טופולוגיה על K ולכן הן שקולות במובן של הערכות. אבל שתיהן מרחיבות את $|\cdot|$ על F שאינה טריוואלית, ולכן שתי הרחבות של $|\cdot|$ על K הן זהות.
קיום: מקרה ארכימדי - בפרק הבא. נניח ש$|\cdot|$ לא ארכימדית, אז $|\cdot|$ דיסקרטית על F לפי ההנחה, ולכן ראינו שקיימת הרחבה לK.
ראינו ש$\langle K,|\cdot|_K\rangle$ שלם.
נוסחה: תהי L/F הרחבת גלואה כך ש$F\subseteq K\subseteq L$. נסמן $l=[L:F]$. אז $l/n=[L:K]$.
תהי $|\cdot|$ ההרחבה היחידה לL. (כאן מניחים שקיימת הרחבה לL וראינו יחידות). לכל איבר $\sigma\in\mathrm{Gal}(L/F)$ יש הערכה $|\cdot|^\sigma$ הנתונה ע"י

$$|x|^\sigma=|\sigma(x)| \qquad (x\in L)$$

מיחידות נובע ש $|x| = |\sigma(x)|$ לכל $x \in L$. מכאן

$$\begin{aligned} \left|N_{L/F}(x)\right| &= \left|\prod_{\sigma\in\mathrm{Gal}(L/F)} \sigma(x)\right| \\ &= \prod_{\sigma\in\mathrm{Gal}(L/F)} |\sigma(x)| \\ &= |x|^l \end{aligned}$$

לבסוף אם $x \in K$ אז

$$\begin{aligned} \left|N_{K/F}(x)\right|^{\frac{l}{n}} &= \left|N_{K/F}(x)\right|^{[L:K]} \\ &= \left|N_{K/F}\left(x^{[L:K]}\right)\right| \\ \underbrace{}_{\substack{x\in K \\ \sigma(x)=x \\ \forall\sigma\in\mathrm{Gal}(L/K)}} &= \left|N_{K/F}\left(N_{L/K}(x)\right)\right| \\ &= \left|N_{L/F}(x)\right| \\ &= |x|^l \end{aligned}$$

לכן $\left|N_{K/F}(x)\right|^{\frac{1}{n}} = |x|$ לכל $x \in K$. ■

11.3 טורים בשדה דיסקרטי שלם

יהי $\langle K, |\cdot| \rangle$ שדה הערכה דיסקרטי (בפרט לא ארכימדי) שלם.

טענה 11.11 (התכנסות טורים): $\sum_{n=1}^{\infty} a_n$ מתכנס $\iff$ $\lim_{n\to\infty} a_n = 0$

הוכחה: $\Longleftarrow$: כמו בחדו"א.

$\Longrightarrow$: יהי $\varepsilon > 0$. יש N כך שלכל $n \geq N$ מתקיים $|a_n| \leq \varepsilon$ ולכן אם $m \geq n \geq N$ אז $\left|\sum_{i=m}^{n} a_i\right| \leq \varepsilon$ לכן סדרת הסכומים החלקיים היא סדרת קושי, ולכן יש לה גבול. ■

הערה 11.12 (תכונות): אם $\sum_{n=1}^{\infty} a_n = a$ אז:

1. $|a| \leq \max_{n=1}^{\infty} |a_n|$

   הוכחה: אכן $|a| \longleftarrow \left|\sum_{i=1}^{m} a_i\right| \leq \max_{i=1}^{m} |a_i|$. ■

2. אם $|a_1| > |a_i|$ לכל $i > 1$ אז $|a| = \left|\sum_{i=1}^{\infty} a_i\right|$

   הוכחה: אכן $|a_1| > \max_{i=2}^{\infty} |a_i| \geq \left|\sum_{i=2}^{\infty} a_i\right|$ ולכן מאי־שוויון המשולש הלא־ארכימדי $\left|\sum_{i=1}^{\infty} a_i\right| = \left|a_1 + \sum_{i=2}^{\infty} a_i\right| = |a_1|$. ■

3. לכל תמורה $\sigma:\mathbb{N}\to\mathbb{N}$ מתקיים $\sum_{i=1}^{\infty}a_{\sigma(i)}=\sum_{i=1}^{\infty}a_i$.

הוכחה: יהי $\varepsilon>0$. יהי N כך שלכל $n\geq N$ מתקיים $|a_n|<\varepsilon$. יהי $N'\geq N$ כך ש $\{a_1,\ldots,a_N\}\subseteq\left\{a_{\sigma(1)},\ldots,a_{\sigma(N')}\right\}$.
אם $n\geq N'$ אז הקבוצות $\{a_1,\ldots,a_n\}$ ו$\left\{a_{\sigma(1)},\ldots,a_{\sigma(n)}\right\}$ מכילות את $\{a_1,\ldots,a_N\}$ ולכן

$$\begin{aligned}\left|\sum_{i=1}^{n}a_i-\sum_{i=1}^{N}a_i\right| &< \varepsilon\\ \left|\sum_{i=1}^{n}a_{\sigma(i)}-\sum_{i=1}^{N}a_i\right| &< \varepsilon\end{aligned}$$

ומכאן $\left|\sum_{i=1}^{n}a_i-\sum_{i=1}^{n}a_{\sigma(i)}\right|<\varepsilon$. ■

4. ניתן גם לחלק את הטור $\sum_{i=1}^{\infty}a_i$ לטור של טורים והסכום לא משתנה.

11.4 טורי "לורן"

טענה 11.13 יהי $\langle K,|\cdot|\rangle$ שדה הערכה שלם ודיסקרטי (ואז גם לא ארכימדי). יהי π ראשוני ותהי $S=\{s\}_{s\in S}\subseteq R_{|\cdot|}$ קבוצת נציגים עם $0\in S$. יהי $x\neq 0$ ונסמן $n=\mathrm{ord}_K(x)$. אז קיים תיאור יחיד

$$x = \sum_{i=n}^{\infty}s_i\pi^i$$

עם $s_i\in S$ לכל i ומתקיים $s_n\neq 0$.

הערה 11.14 בכיוון ההפוך, טור מהצורה $\sum_{i=n}^{\infty}s_i\pi^i$ עם $s_i\in S$ לכל i ו$s_n\neq 0$ מתאר $x\in K^{\times}$ עם $n=\mathrm{ord}_K x$.

הוכחה: ברור שהטור מתכנס (כי $s\in S\implies |s|\leq 1$) ומתקיים $|s_n\pi^n|=|\pi|^n$ (כי $S\ni s_n\neq 0$ ולכן $|s_n|=1$) ולכל $i>n$ מתקיים $\left|s_i\pi^i\right|<|\pi|^i<|\pi|^n=|s_n\pi^n|$ ולכן $|x|=|s_n\pi^n|=|\pi|^n$, ומכאן $\mathrm{ord}_K x=n$. ■

הוכחה: (של הטענה): יחידות: נניח $\sum_{i=l}^{\infty}(s_i-\widetilde{s_i})\,\pi^i=0$, כאשר $s_i,\widetilde{s_i}\in S$ לכל i. צריך להוכיח ש$s_i=\widetilde{s_i}$ לכל i. הוכחה בדרך השלילה: אפשר להניח ש$s_l\neq\widetilde{s_l}$ ואז $|s_l-\widetilde{s_l}|=1$. כמו קודם, נותר

$$0 = \left|\sum_{i=l}^{\infty}(s_i-\widetilde{s_i})\,\pi^i\right|=|\pi|^l$$

סתירה.

קיום: $\frac{x}{\pi^n}\in U$ ולכן יש $0\neq s_n\in S$ עם $\frac{x}{\pi^n}-s_n\in P=\pi R$. כלומר

$$x_1 = x-s_n\pi^n\in\pi^{n+1}R$$

ואז יש $s_{n+1}\in S$ עם

$$x-s_n\pi^n-s_{n+1}\pi^{n+1}\quad\in\quad\pi^{n+2}R$$

וממשיכים בצורה הזאת. ■

11.5 השלמה

טענה 11.15 יהי $\langle K,|\cdot|\rangle$ שדה הערכה, אז קיים שדה הערכה $\left\langle K',|\cdot|'\right\rangle$ שלם ושיכון של שדות $i:K\hookrightarrow K'$ כך ש $i\left(K\right)$ צפוף בK' וכך שi איזומטריה, כלומר $|i\left(x\right)|'=|x|$ לכל $x\in K$.
בנוסף, אם $\left\langle K'',|\cdot|''\right\rangle$ שדה הערכה שלם ו$j:K\hookrightarrow K''$ שיכון איזומטרי של שדות, אז קיים שיכון רציף יחיד $\varphi:K'\to K''$ של שדות כך ש $j=\varphi\circ i$ וφ איזומטריה.

הגדרה 11.16 $\left\langle K',|\cdot|'\right\rangle$ כנ"ל נקרא ההשלמה של $\langle K,|\cdot|\rangle$.

מסקנה 11.17 אם $\left\langle K_1',|\cdot|_1'\right\rangle$ השלמה נוספת עם שיכון $i_1:K\hookrightarrow K_1'$ איזומטרי, אז יש שיכון רציף $f:K'\to K_1'$ כך ש$i_1=f\circ i$ ואז f איזומורפיזם איזומטרי.

הוכחה: (של הטענה): הטענה אינווריאנטית ביחס למעבר מ$|\cdot|$ להערכה שקולה $|\cdot|^\rho$ (כאשר $\rho>0$), לכן אפשר להניח ש$|2|\leq 2$ ואז נובע שכל ההערכות הנידונות הן ערכים מוחלטים, והמרחבים הופכים למטריים. במצב זה, ההוכחה סטנדרטית. ■

<u>(תכונות ההשלמה):</u> נתייחס ל$i:K\hookrightarrow K'$ כהכלה $K\subseteq K'$ ונסמן $|z|=|z|'$ (לכל $z\in K'$).

הערה 11.18 המספר $C_{|\cdot|}=\max\left\{1,|2|\right\}$ לא משתנה, לכן:

1. K לא ארכימדי $\iff$ K' לא ארכימדי
2. $|\cdot|$ ערך מוחלט על K $\iff$ $|\cdot|$ ערך מוחלט על K'.

כעת נניח שK לא ארכימדי ולכן K' לא ארכימדי.

הערה 11.19 <u>חבורת ההערכה:</u> ברור ש $\left|\left(K'\right)^\times\right|=|K^\times|$ כי לכל $z\in\left(K'\right)^\times$ קיים $x\in K$ עם $|x-z|<|z|$ ולכן $|x|=|z|$ (ובפרט $x\neq 0$).

מסקנה 11.20 K דיסקרטי $\iff$ K' דיסקרטי ובמקרה זה מתקיים: π ראשוני של K $\iff$ π ראשוני של K'. (כאשר $\pi\in K$)

הערה 11.21 <u>(שדה השארית):</u> נסמן בR', U', P' את חוג השלמים, ההפיכים והאידאל המקסימלי בK'. אז $R=R'\cap K$, $P=P'\cap K$, $U=U'\cap K$ ולכן יש שיכון

$$\overline{K}=R/P\quad\hookrightarrow\quad R'/P'=\overline{K'}$$

וזהו איזומורפיזם. לכן נכתוב $\overline{K}=\overline{K'}$.

הוכחה: אכן, די להוכיח שהשיכון הוא על (הומומורפיזם של שדות הוא תמיד חד־חד־ערכי): נבדוק איבר $0_{\overline{K'}} \neq z + P' \in \overline{K'}$, עם $z' \in R'$. אז $z \notin P'$ ולכן $|z| = 1$. יהי $x \in K$ עם $|x - z| < 1$. אז $|x| = |z| = 1$ ו־$x + P' = z + P'$ ו $\varphi(x + P) = x + P'$. ■

מסקנה 11.22 אם $S \subseteq R$ קבוצת נציגים של $\overline{K}$, אז S גם קבוצת נציגים של $\overline{K'}$.

הערה 11.23 (צפיפות): לכל $z \in K'$ יש סדרה $z \longrightarrow x_n \in K$ עם $|x_n| = |z|$.

הוכחה: אפשר להניח ש $|z| \neq 0$ ולקחת סדרה כך ש $|x_n - z| < |z|$ לכל n ואז $|x_n| = |z|$.
■

הערה 11.24 בפרט U צפוף ב־U', P צפוף ב־P', R צפוף ב־R'.

11.6 $\mathbb{Q}_p$

הגדרה 11.25 $\langle \mathbb{Q}_p, |\cdot| \rangle$ הוא ההשלמה של $\left\langle \mathbb{Q}, |\cdot|_p \right\rangle$. (כאשר p ראשוני)

הערה 11.26 (תכונות):

1. חבורת ההערכה היא
$$\left|\mathbb{Q}_p^\times\right|_p \quad = \quad \left|\mathbb{Q}^\times\right|_p = \left\{p^{-n}\right\}_{n=-\infty}^{\infty}$$

2. חוג השלמים (חוג ההערכה) של $\mathbb{Q}_p$ מסומן ב־$\mathbb{Z}_p$. $\mathbb{Z}_p$ הוא הסגור של חוג השלמים של $\mathbb{Q}$ ביחס ל־$|\cdot|_p$ ולכן גם הסגור של $\mathbb{Z}$ ב־$\mathbb{Q}_p$.

3. יש הומומורפיזם יחיד של חוגים שהינו איזומורפיזם של שדות
$$\mathbb{Z}/p\mathbb{Z} \quad \xrightarrow{\sim} \quad \overline{\mathbb{Q}} = \overline{\mathbb{Q}_p}$$
כי ראינו ש־$\overline{\mathbb{Q}} = \overline{\mathbb{Q}_p}$, וראינו בעבר כי $S = \{0, 1, \ldots, p-1\}$ היא קבוצת נציגים של $\overline{\mathbb{Q}}$. לכן S הנ"ל קבוצת נציגים של $\overline{\mathbb{Q}_p}$.

4. p הוא ראשוני של $\mathbb{Q}_p$ (כי הוא ראשוני של $\mathbb{Q}_p$).

מסקנה 11.27 לכל $x \in \mathbb{Q}_p^\times$ יש תיאור יחיד ע"י
$$x \quad = \quad \sum_{i=n}^{\infty} a_i p^i$$
עם $a_i \in \{0, 1, \ldots, p-1\}$ (לכל i) ו־$a_n \neq 0$. ואז $n = \mathrm{ord}_{\mathbb{Q}_p}(x)$. כלומר $|x| = \frac{1}{p^n}$. כמו כן $n \geq 0 \iff x \in \mathbb{Z}_p$.

11.7 שדות מקומיים

הגדרה 11.28 שדה p־אדי הוא שדה הערכה לא ארכימדי $\langle F, |\cdot| \rangle$ כך ש

1. $|\cdot|$ דיסקרטית (ולא טריוואלית).
2. שדה השארית סופי (ואז $p = \mathrm{char}\overline{F}$)
3. ההערכה $|\cdot|$ שלמה

הגדרה 11.29 שדה מקומי הוא $\mathbb{R}$, $\mathbb{C}$ או שדה p־אדי.

הגדרה 11.30 (גרסה שנייה): שדה מקומי הוא שדה טופולוגי F כך שF איזומורפי כשדה טופולוגי ל$\mathbb{R}$, $\mathbb{C}$ או שדה p־אדי.

הגדרה 11.31 (גרסה שלישית): שדה מקומי הוא שדה טופולוגי קומופקטי מקומית עם טופולוגיה לא דיסקרטית. (Weil, Ramakrishnan-Valenza)

הערה 11.32 (מציין): יהי F שדה מקומי.

1. אם $\mathrm{char}F = p > 0$ אז $\mathrm{char}F = \mathrm{char}\overline{F} = p$. במקרה זה F שדה p־אדי (כי $\mathbb{R}$ ו$\mathbb{C}$ לא ייתכנו). מצב זה נקרא מצב של "מציינים שווים" ("Equal character"), או מצב של שדות פונקציות ("Function field case") במצב זה ניתן לקחת קבוצת נציגים שהיא תת־שדה של F.

הערה 11.33 (הדוגמה): אם נקח שדה סופי L ומשתנה z ונתייחס לטורי לורן $\sum_{i=n}^{\infty} l_i z^i$ כאשר $l_i \in L$.

2. אם $\mathrm{char}F = 0$. כאן ייתכן
   (א) $F = \mathbb{R}$ או $F = \mathbb{C}$
   (ב) F שדה p־אדי, $\mathrm{char}F = 0 \neq p = \mathrm{char}\overline{F}$. מקרה זה נקרא "Unequal characteristic case" או "Number field case".

11.8 קומפקטיות מקומית

טענה 11.34 כל שדה מקומי הוא קומפקטי מקומית.

הוכחה: ל$\mathbb{C}$, $\mathbb{R}$ זה ידוע.
נניח ש$\langle F, |\cdot| \rangle$ שדה p־אדי. מאחר ש $\{x + P^n\}_{n \in \mathbb{Z}}$ הוא בסיס לסביבות של x, די להוכיח שכל $x + P^n$ קומפקטית, ולכן די להוכיח שP^n קומפקטית לכל $n \in \mathbb{Z}$. כעת $P^n = \pi^n R$ (כאשר π ראשוני וR חוג השלמים) ו$\pi^n : F \to F$ הומיאומורפיזם, לכן די להוכיח ש $R = \{x \mid |x| \leq 1\}$ קומפקטי. תהי S קבוצת נציגים. אז S סופית. יש העתקה על:

$$\begin{aligned} f : S^{\mathbb{N}} &\to R \\ s = \{s_i\}_{i=0}^{\infty} &\mapsto f(s) = \sum_{i=0}^{\infty} s_i \pi^i \end{aligned}$$

די להוכיח שf רציפה (כי $S^{\mathbb{N}}$ קומפקטית). אכן תהי $\tilde{s}=\{\widetilde{s_i}\}\in S^{\mathbb{N}}$ ויהי $\varepsilon>0$. יש N כך ש $|\pi|^N<\varepsilon$ ולכל $s=\{s_i\}_{i=1}^{\infty}$ עם $s_0=\widetilde{s_0},\ldots,s_N=\widetilde{s_N}$. מתקיים

$$|f(s)-f(\tilde{s})| = \left|\sum_{i=N+1}^{\infty}(s_i-\widetilde{s_i})\pi^i\right|\leq|\pi|^{N+1}<\varepsilon$$

ולכן f רציפה. ■

מסקנה 11.35 יהי $\langle F,|\cdot|\rangle$ שדה מקומי.

1. יש בF סדרה צפופה בF (פולינומים עם חזקות חיוביות ושליליות בπ).
2. יש לF בסיס בן מנייה לטופולוגיה, למשל ניתן לקחת קבוצות מהצורה $d+P^n$ עם d בקבוצה צפופה ו$n\geq 0$ ואז קבוצות אלה גם קומפקטיות.
3. כל קבוצה פתוחה היא σ־קומפקטית (איחוד סופי או בן מניה של קבוצות קומפקטיות).

הערכה מנורמלת יהי $\langle F,|\cdot|\rangle$ שדה p־אדי, נסמן $q=\#\overline{F}=\#(R/P)$. אז קיים $k\geq 1$ כך ש$p=q^k$. ניתן לנרמל את ההערכה $|\pi|=\frac{1}{q}$ (π ראשוני) ואז אומרים ש$|\cdot|$ מנורמלת. (זהו גם המודולוס של π לפי מידת האר).

12 הערכות שלמות ארכימדיות

12.1 תזכורת על אלגבראות בנך

הגדרה 12.1 אלגברת בנך היא מרחב בנך $\langle A,\|\cdot\|\rangle$ מעל $\mathbb{C}$ עם מכפלה בילינארית

$$\cdot : A\times A \rightarrow A$$

ואסוציאטיבית כך ש

$$(x,y\in A)\qquad \|xy\|\leq\|x\|\cdot\|y\|$$

נניח גם שלA יש יחידה $1=1_A$ ו$\|1\|=\|1_A\|=1$.

הגדרה 12.2 (ספקטרום): לכל $a\in A$ הספקטרום של a מוגדר ע"י

$$\sigma(a) = \{\lambda\in\mathbb{C}\mid \lambda 1_A-a \text{ is not invertible in } A\}$$

משפט 12.3 לכל $a\in A$, $\sigma(a)\neq\emptyset$.

מסקנה 12.4 אם A אלגברת בנך עם חילוק (כלומר כל $a\neq 0$ הפיך) אז $A=\mathbb{C}\cdot 1_A$ (כולל שוויון בנורמות) ולכן $A=\mathbb{C}$.

הוכחה: (של המשפט): בדרך השלילה, נניח ש$\lambda \cdot 1_A - a$ הפיך לכל λ. נסתכל על הפונקציה

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & A \\ \lambda & \mapsto & (\lambda 1_A - a)^{-1} \end{array}$$

ולכל $\varphi \in A^*$ נסתכל על הפונקציה

$$\begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ \varphi & \to & \varphi\left((\lambda 1_A - a)^{-1}\right) \end{array}$$

נוכיח שהפונקציה $\varphi\left((\lambda 1_A - a)^{-1}\right)$ הולומורפית על כל $\mathbb{C}$ ומתקיים $\lim_{|\lambda|\to\infty} \varphi\left((\lambda 1_A - a)^{-1}\right) = 0$, ואז ממשפט ליוביל $\varphi\left((\lambda 1_A - a)^{-1}\right) = 0$ לכל $\lambda \in \mathbb{C}$ ולכל $\varphi \in A^*$. נקבל סתירה למשל כי $a^{-1} \neq 0$ ויש $\varphi \in A^*$ כך ש$\varphi\left(a^{-1}\right) \neq 0$.

<u>הולמורפיות:</u> יהי $z \in \mathbb{C}$.

$$\begin{aligned} ((\lambda + z) 1_A - a)^{-1} &= \left[\left(1_A + z(\lambda 1_A - a)^{-1}\right)(\lambda 1_A - a)\right]^{-1} \\ &= (\lambda 1_A - a)^{-1}\left(1_A + z(\lambda 1_A - a)^{-1}\right)^{-1} \end{aligned}$$

נקח $|z| < \frac{1}{\left\|(\lambda 1_A - a)^{-1}\right\|}$ ואז

$$(\lambda 1_A - a)^{-1}\left(1 + z(\lambda 1_A - a)^{-1}\right)^{-1} = (\lambda 1_A - a)^{-1}\left(1_A - z(\lambda 1_A - a)^{-1} + z^2(\lambda 1_A - a)^2 - \dots\right)$$

וע"י הפעלת φ נקבל ש $\varphi\left(((\lambda + z) 1_A - a)^{-1}\right)$ נתונה ע"י טור חזקות בz בעיגול לעיל.

<u>גבול:</u> ניקח $|\lambda| > 2\|a\|$.

$$\begin{aligned} (\lambda 1_A - a)^{-1} &= \left(\lambda\left(1_A - \lambda^{-1} a\right)\right)^{-1} \\ &= \lambda^{-1}\left(1_A - \lambda^{-1} a\right)^{-1} \end{aligned}$$

מאחר ש $\left\|\lambda^{-1} a\right\| < \frac{1}{2}$ נקבל

$$\left\|\left(1_A - \lambda^{-1} a\right)^{-1}\right\| = \left\|1_A + \lambda^{-1} a + \left(\lambda^{-1} a^1\right)^2 + \dots\right\| \leq 2$$

ולכן $(\lambda 1_A - a)^{-1} \leq \frac{2}{|\lambda|}$ (ל$\lambda > 2\|a\|$), ולכן $\lim_{|\lambda|\to\infty} (\lambda 1_A - a)^{-1} = 0$ ומכאן $\varphi\left((\lambda 1_A - a)^{-1}\right) \xrightarrow[|\lambda|\to\infty]{} 0$. ■

מסקנה 12.5 יהי $\langle K, |\cdot|_K \rangle$ שדה ארכימדי שלם ונניח כי $K \subseteq \mathbb{C}$ ושההערכה $|\cdot|_K$ מצומצמת ל$\mathbb{C}$ היא הערך מוחלט הרגיל על $\mathbb{C}$. אז $K = \mathbb{C}$.

הוכחה: אכן, הצמצום של $|\cdot|_K$ על $\mathbb{Q}$ הוא הערך המוחלט הרגיל, ולכן $|\cdot|_K$ ערך מוחלט ולכן K אלגברת בנך (מעל $\mathbb{C}$). ■

למה 12.6 תהי $|\cdot|$ הערכה של שדה K שלם ונניח שלמשוואה $x^2+1=0$ אין פתרון בK. תהי $\Gamma=K+iK$ ההרחבה ע"י הוספת i המקיימת $i^2+1=0$. נגדיר

$$|\cdot|_\Gamma:\Gamma\quad\longrightarrow\quad[0,\infty)$$

על ידי

$$|x+yi|_\Gamma=\sqrt{|x^2+y^2|}\qquad(x,y\in\Gamma)$$

אז $|\cdot|_\Gamma$ הערכה של Γ המרחיבה את $|\cdot|$.

הוכחה: אפשר להחליף את $|\cdot|$ בהערכה שקולה, ולכן אפשר להניח ש$|\cdot|$ ערך מוחלט על K.
<u>צמצום על K:</u> $|x|_\Gamma=|x+i0|_\Gamma=\sqrt{|x^2+0^2|}=\sqrt{|x|^2}=|x|$.
<u>נורמה 0:</u> נניח ש $|x+iy|_\Gamma=0$ אז $x^2+y^2=0$. אם למשל $y\neq 0$ נקבל $\left(\frac{x}{y}\right)^2+1=0$. סתירה. לכן $y=0$ ואז $x=0$.
<u>כפליות:</u>

$$\begin{aligned}|(x+iy)(s+it)|_\Gamma^2 &= |(xs-yt)+i(xt+ys)|_\Gamma^2\\ &= \left|(xs-yt)^2+(xt+ys)^2\right|\\ &= \left|x^2s^2+y^2t^2+x^2t^2+y^2s^2\right|\\ &= \left|\left(x^2+y^2\right)\left(s^2+t^2\right)\right|\\ &= \left|x^2+y^2\right|\cdot\left|s^2+t^2\right|\\ &= |x+iy|_\Gamma^2\cdot|s+it|_\Gamma^2\end{aligned}$$

כעת נוכיח ש$|\cdot|_\Gamma$ הערכה. לפי ארטין, צריך להוכיח כי

$$\sup_{\substack{\gamma\in\Gamma\\|\gamma|_\Gamma\le 1}}|\gamma+1|_\Gamma\quad<\quad\infty$$

נסמן $\gamma=a+ib$ ($a,b\in K$), אז $\gamma+1=a+1+ib$. לכן צריך להוכיח

$$\sup_{\substack{|a^2+b^2|\le 1\\a,b\in K}}\left|(a+1)^2+b^2\right|\quad<\quad\infty$$

מתקיים

$$\begin{aligned}\left|(a+1)^2+b^2\right| &= \left|a^2+b^2+1+2a\right|\\ &\le \left|a^2+b^2\right|+|1|+|2|\,|a|\\ &\le 1+1+|2|\,|a|\\ &= 2+|2|\,|a|\end{aligned}$$

לכן די להוכיח כי

$$\sup_{\substack{a,b\in K\\|a^2+b^2|\le 1}}|a|\quad<\quad\infty$$

נוכיח זאת בדרך השלילה: נניח $\left|a_n^2+b_n^2\right|\leq 1$ אבל $|a_n|\underset{n\to\infty}{\longrightarrow}\infty$. נציב $x_n=\frac{b_n}{a_n}$ ונקבל

$$\left|x_n^2+1\right| = \left|\left(\frac{b_n}{a_n}\right)^2+1\right|=\left|\frac{a_n^2+b_n^2}{a_n^2}\right|\leq\frac{1}{\left|a_n^2\right|}\longrightarrow 0$$

ולכן $\lim_{n\to\infty}\left(x_n^2+1\right)=0$.
ע"י מעבר לתת־סדרה סדרה, אפשר להניח כי $\left|x_n^2+1\right|\leq\frac{1}{2\cdot 4^n}$ ואז

$$\begin{aligned}|x_{n+1}-x_n|\,|x_{n+1}+x_n| &= \left|x_{n+1}^2-x_n^2\right| \\ &= \left|\left(x_{n+1}^2+1\right)-\left(x_n^2+1\right)\right| \\ &\leq \left|x_{n+1}^2+1\right|+\left|x_n^2+1\right| \\ &\leq \frac{1}{4^n}\end{aligned}$$

לכאן אחד מ $|x_n\pm x_{n+1}|$ קטן או שווה מ$\frac{1}{2^n}$. ע"י שינוי הסימן של x_{n+1} (אם יש צורך), אפשר להניח ש $|x_{n+1}-x_n|\leq\frac{1}{2^n}$. מאחר ש$|\cdot|$ ערך מוחלט על K, נקבל ש

$$\lim_{n,m\to\infty}|x_n-x_m| = 0$$

מאחר שK שלם קיים $\lim_{n\to\infty}x_n=x\in K$ ומכך ש$\lim_{n\to\infty}\left(x_n^2+1\right)=0$ נובע ש$x^2+1=0$. סתירה. ■

משפט 12.7 יהי $\left\langle K,|\cdot|_K\right\rangle$ שדה ארכימדי שלם. נניח כי $|2|_K=2$. אז קיים איזומורפיזם שומר הערכות $K\xrightarrow{\cong}\mathbb{R}$ או $K\xrightarrow{\cong}\mathbb{C}$. (כאשר $\mathbb{R}$ ו$\mathbb{C}$ עם ערכים מוחלטים רגילים)

הערה 12.8 אם $\left\langle K,|\cdot|_K\right\rangle$ שדה ארכימדי אז $|2|_K>1$ ואז קיים $\rho>0$ (יחיד) עם $|2|_K^\rho=2$, כלומר $|\cdot|_K$ שקולה להערכה (יחידה) המקיימת את תנאי המשפט.

הוכחה: (של המשפט): הצמצום $|\cdot|_K\restriction_{\mathbb{Q}}$ זהה לערך המוחלט הרגיל על $\mathbb{Q}$. ראינו גם ש$|\cdot|_K$ ערך מוחלט על K (כי $C_{|\cdot|}=\max\left(1,|2|_K\right)=2\leq 2$). לכן K הופך למרחב מטרי שלם. מכאן נובע שניתן להרחיב את השיכון האיזומטרי $\mathbb{Q}\subseteq K$ לשיכון איזומטרי (שומר הערכות) $\mathbb{R}\subseteq K$ כאשר $\mathbb{R}$ עם הערך המוחלט הרגיל.

מקרה ראשון: K מכיל פתרון למשוואה $x^2+1=0$, אז יש איזומורפיזם של שדות $K\supseteq\mathbb{R}\oplus\mathbb{R}i\cong\mathbb{C}$. מאחר ו$\mathbb{C}/\mathbb{R}$ ספרבילית סופית, יש להערכה של $\mathbb{R}$ הרחבה יחידה להערכה של $\mathbb{C}$ (עם הערך המוחלט הרגיל). לכן $\mathbb{C}\subseteq K$ שיכון שומר הערכות. לבסוף K אלגברת בנך (כי ארכימדי שלם) ושדה, ולכן $K=\mathbb{C}$.

מקרה שני: אין פתרון ל$x^2+1=0$ בK. נגדיר הרחבה Γ/K ע"י $\Gamma=K(i)$ עם i המקיים $i^2+1=0$. Γ/K ספרבילית סופית (K שלם), ולכן יש ל$|\cdot|_K$ הרחבה להערכה $|\cdot|_\Gamma$ על Γ. מתקיים $|2|_\Gamma=|2|_K=2$ ולכן $|\cdot|_\Gamma$ ערך מוחלט על Γ. לכן Γ מרחב נורמי מעל K, ולכן Γ שלם. נסמן $\Gamma\supseteq\mathbb{R}\oplus i\mathbb{R}=\mathbb{C}$. אז מהחלק הראשון נובע ש$\mathbb{C}\subseteq\Gamma$ (כולל שוויון בהערכה). לבסוף $\Gamma\supsetneqq K\supseteq\mathbb{R}$ ו$\dim_{\mathbb{R}}(\Gamma)=2$ ולכן $\dim_{\mathbb{R}}(K)=1$ ו$K=\mathbb{R}$. ■

13 מידת האר

(מבוסס על Rudin - Real and Complex Analysis).

13.1 σ־אלגברה

הגדרה 13.1 (σ־אלגברה): תהי X קבוצה אוסף Σ של תת־קבוצות של X נקרא σ־אלגברה (בX) אם:

1. $\emptyset, X \in \Sigma$
2. $A \in \Sigma \implies X \setminus A \in \Sigma$
3. $A_n \in \Sigma$ ($n = 1, 2, \ldots$) $\implies \bigcup_{n=1}^{\infty} A_n \in \Sigma$

הערה 13.2 (תכונה): לכל אוסף של תת־קבוצות של X, Ω, יש σ־אלגברה המכילה את Ω ומוכלת בכל σ־אלגברה המכילה את Ω, הנקראת הσ־אלגברה הנוצרת ע"י Ω.

הגדרה 13.3 (קבוצת בורל): יהי X מרחב טופולוגי. הσ־אלגברה הנוצרת ע"י אוסף התת־קבוצות הפתוחות של X נקראת הσ־אלגברה של קבוצות <u>בורל</u> של X ומסומנת $\mathcal{B}(X)$.

טענה 13.4 יהי X מרחב טופולוגי, תהי $\Gamma \subseteq X$ בורל. אז שלושת האוספים הבאים של Γ זהים:

1. $\mathcal{B}(\Gamma)$
2. $\{E \cap \Gamma \mid E \in \mathcal{B}(X)\}$
3. $\{F \subseteq \Gamma \mid F \in \mathcal{B}(X)\}$

בפרט אם $A \in \mathcal{B}(\Gamma)$ אז $A \in \mathcal{B}(X)$. (כי הקבוצה הראשונה זהה לקבוצה השלישית)

הוכחה: נסמן בΣ את אוסף כל התת־קבוצות $A \subseteq X$ כך ש$A \cap \Gamma \in \mathcal{B}(\Gamma)$. אז Σ היא σ־אלגברה בX. כמו כן, כל קבוצה פתוחה $\mathcal{O} \subseteq X$ שייכת לΣ ולכן $\mathcal{B}(X) \subseteq \Sigma$. מכאן הקבוצה ב2 חלקית לקבוצה ב1. כעת, נשים לב כי 3 היא σ־אלגברה בΓ (כי $\Gamma \in \mathcal{B}(X)$). כמו כן, כל קבוצה פתוחה $\mathcal{O} \subseteq \Gamma$ של Γ נמצאת ב3: אכן קיימת קבוצה פתוחה $U \subseteq X$ כך ש$\mathcal{O} = U \cap \Gamma$ ולכן $\mathcal{O} \in \mathcal{B}(X)$ (כי $U, \Gamma \in \mathcal{B}(X)$). מכאן $1 = \mathcal{B}(\Gamma) \subseteq 3$.
לבסוף, אם לבסוף אם F ב3 אז $F \in \mathcal{B}(X)$ ו$F = F \cap \Gamma$ ולכן $3 \subseteq 2$. ■

13.2 מידה ואינטגרציה

הגדרה 13.5 תהי Σ σ־אלגברה על X. מידה על Σ היא פונקציה $\mu : \Sigma \to [0, \infty]$ כך ש

1. $\mu(\emptyset) = \emptyset$
2. אם $A_1, A_2, A_3, \dots \in \Sigma$ עם $A_i \cap A_j = \emptyset$ (לכל $i \neq j$) אז $\mu\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mu(A_i)$.

מסמנים $\langle X, \Sigma, \mu \rangle$ מרחב מידה.

הגדרה 13.6 (מינוח) מידת בורל על מרחב טופולוגי X היא מידה על $\mathcal{B}(X)$.

הגדרה 13.7 יהי $\langle X, \Sigma, \mu \rangle$ מרחב מידה. פונקציה פשוטה היא פונקציה מהצורה

$$f = \sum_{i=1}^{n} a_i \mathrm{Char}_{A_i}$$

כאשר $A_i \in \Sigma$ (זרות לזו לזה) ו$0 \le a_i < \infty$ (לכל i)

במצב זה מסמנים

$$\int_X f d\mu = \int_X f dx = \sum_{i=1}^{n} a_i \mu(A_i)$$

כאשר מפרשים $0 = 0 \cdot \infty = \infty \cdot 0$.

הגדרה 13.8 (פונקציה מדידה): תהי Σ σ־אלגברה על X וY מרחב טופולוגי. פונקציה $f : X \to Y$ נקראת מדידה אם לכל $\mathcal{O} \subseteq Y$ פתוחה מתקיים $f^{-1}(\mathcal{O}) \in \Sigma$.

הערה 13.9 (תכונות):

1. אם f מדידה וh רציפה אז $h \circ f$ מדידה.
2. פעולות אלגבריות וגבולות שומרים על פונקציות מדידות. (למשל $f : X \to \mathbb{R}$)

הערה 13.10 נתייחס ל $[0,\infty] = [0,\infty) \cup \{\infty\}$ (קומפקטיפיקציה חד נקודתית של $[0,\infty)$) ויש הומיאומורפיזם

$$\left[0, \frac{\pi}{2}\right] \to [0,\infty] \quad : \quad \begin{cases} 0 \le x < \frac{\pi}{2} & \mapsto \tan x \\ \frac{\pi}{2} & \mapsto \infty \end{cases}$$

טענה 13.11 תהי $f : X \to [0,\infty]$ מדידה. אז יש פונקציות פשוטות על X כך ש

1. $0 \le s_1 \le s_2 \le \cdots \le f$
2. $\lim_{n\to\infty} s_n(x) = f$ לכל $x \in X$

הוכחה: ראה Rudin - Real and Complex Analysis עמוד 15. ■

הגדרה 13.12 תהי $f : X \to [0,\infty]$ מדידה. אז

$$[0,\infty] \ni \int_X f d\mu = \sup\left\{ \int_X s d\mu \mid 0 \le s \le f \mid s \text{ is a simple function} \right\}$$

הערה 13.13 (תכונות):

1. $\int cf = c\int f$
2. $\int (f+g) = \int f + \int g$
3. $f \geq 0 \implies \int f \geq 0$

הגדרה 13.14 תהי $f : X \to \mathbb{C}$, אז f אינטגרבילית אם f מדידה ו $\int |f| < \infty$.

הערה 13.15 (תכונה): קיימת פונקציה לינארית אחת ויחידה $f \mapsto \int_X f d\mu$ המוגדרת על פונקציות אינטגרביליות כך שאם $f \geq 0$, ההגדרה תואמת למה שהיה קודם.

משפט 13.16 (ההתכנסות המונוטונית של לבג): אם $\langle X, \Sigma, \mu \rangle$ מרחב מידה ו $0 \leq f_n : X \to [0, \infty]$ מדידות ($n = 1, 2, \ldots$) עם

$$0 \leq f_1 \leq f_2 \quad \leq \quad \ldots$$

אז $f := \lim_{n\to\infty} f_n$ מדידה ומתקיים $\int f d\mu = \lim_{n\to\infty} \int f_n d\mu$.

הגדרה 13.17 (סימון): אם $E \subseteq X$ מדידה אז $\int_E f d\mu = \int_X f \cdot \mathrm{char}_E d\mu$.

13.3 מרחבים קומפקטיים מקומית (כולם האוסדורף)

יהי X מרחב קומפקטי מקומית (האוסדורף).

הגדרה 13.18

1. אם $f : X \to \mathbb{C}$ אז $\mathrm{supp} f$ הוא הסגור של הקבוצה $\{x \in X \mid f(x) \neq 0\}$.
2. אוסף הפונקציות הרציפות $\varphi : X \to \mathbb{C}$ עם תומך קומפקטי מסומן $C_c(X)$. נסמן גם

$$C_c^+(X) \quad = \quad \{\varphi \in C_c(X) \mid \varphi \geq 0\}$$

3. הסימון $K \prec f$ אומר ש $K \subseteq X$ קומפקטית, $f \in C_c^+(X)$ ו $0 \leq f \leq 1$ ו $f\restriction_K = 1$.
4. הסימון $f \prec V$ אומר ש $V \subseteq X$ פתוחה, $f \in C_c^+(X)$, $0 \leq f \leq 1$ ו $\mathrm{supp} f \subseteq V$
5. $K \prec f \prec V \iff K \prec f \ , \ f \prec V$.

משפט 13.19 (הלמה של אוריסון): יהי X קומפקטי מקומית, $V \subseteq X$ פתוחה, $K \subseteq V$ קומפקטית. אז קיימת $f \in C_c^+(X)$ עם $K \prec f \prec V$. (ראה גם Rudin עמוד 39)

מסקנה 13.20 באותם תנאים קיימת $K \subseteq U \subseteq \overline{U} \subseteq V$ כך ש $\overline{U}$ קומפקטית, U פתוחה, למשל $U = \left\{f(x) > \frac{1}{2}\right\}$.

למה 13.21 יהי X מרחב האוסדורף קומפקטי מקומית ונניח שכל קבוצה פתוחה בX היא σ־קומפקטית. יהי $\mathcal{L}$ האוסף הקטן ביותר של פונקציות $f : X \to [0, \infty]$ המקיים:

1. $C_c^+(X) \subseteq \mathcal{L}$

2. אם $f_i \in \mathcal{L}$ ו $0 \le f_1 \le f_2 \le \dots$ אז $\lim_{i\to\infty} f_i \in \mathcal{L}$

3. אם $f_i \in \mathcal{L}$ ($i = 1, 2, \dots$) ואם קיימת $\varphi \in C_c^+(X)$ כך ש $0 \le \dots \le f_2 \le f_1 \le \varphi$ אז $\lim_{i\to\infty} f_i \in \mathcal{L}$

אז $\mathcal{L}$ מורכב מכל הפונקציות המדידות בורל $f : X \to [0, \infty]$.

הוכחה: ראשית $\mathcal{L}$ קיים: לוקחים את כל אוספי הפונקציות המדידות מX ל$[0,\infty]$ המקיימות את תכונות הטענה. זהו אוסף לא ריק. לוקחים את חיתוך כל האוספים האלה וזהו $\mathcal{L}$. בפרט נובע שכל איבר של $\mathcal{L}$ הוא פונקציה מדידה בורל.

נוכיח את הכיוון ההפוך: לכל קבוצה פתוחה $\mathcal{O}$ יש תיאור $\mathcal{O} = \bigcup_{i=1}^{\infty} K_i$ עם K_i קומפקטית. תהי $f_0 = 0$ ולכל i, תהי

$$(\mathrm{supp} f_{i-1}) \cup K_1 \cup \ldots \cup K_{i-1} \prec f_i \quad \prec \quad \mathcal{O}$$

אז $f_1 \le f_2 \le \dots$ שייכות ל $C_c^+(X)$ ולכן ל$\mathcal{L}$. לכן $\mathrm{Char}_{\mathcal{O}} = \lim_{i\to\infty} f_i \in \mathcal{L}$. בפרט $1 \in \mathcal{L}$. (כאשר 1 פונקציה קבועה על X)

כמו כן, לכל $0 < a < \infty$ מתקיים כי הקבוצה $a\mathcal{L}$ מקיימת את התכונות של הלמה, ולכן $\mathcal{L} \subseteq a\mathcal{L}$. מאותה סיבה $\mathcal{L} \subseteq a^{-1}\mathcal{L}$ ומכאן $a\mathcal{L} \subseteq \mathcal{L}$ ולכן $a\mathcal{L} = \mathcal{L}$. כלומר, לכל $g \in \mathcal{L}$ ו$0 < a < \infty$ מתקיים $ag \in \mathcal{L}$.

נראה שלכל $f, g \in \mathcal{L}$ מתקיים $\min(f, g) \in \mathcal{L}$: לכל פונקציה $g : X \to [0, \infty]$ נסמן ב$\mathcal{L}_g$ את אוסף הפונקציות $f : X \to [0, \infty]$ כך ש $\min(f, g) \in \mathcal{L}$. אז $\mathcal{L}_g$ מקיימת את 2 ו3. אם $g \in C_c^+(X)$ אז $\mathcal{L}_g$ מקיימת גם את 1. לכן $\mathcal{L} \subseteq \mathcal{L}_g$ כאשר $g \in C_c^+(X)$, כלומר אם $g \in C_c^+(X)$ ו $f \in \mathcal{L}$ אז $\min(f, g) \in \mathcal{L}$.

לכן ל $g \in \mathcal{L}$ ו $f \in C_c^+(X)$ אז $\min(f, g) \in \mathcal{L}$. מכאן שעבור $g \in \mathcal{L}$, מתקיים כי $\mathcal{L}_g$ מקיימת גם את 1, ומכאן $\mathcal{L} \subseteq \mathcal{L}_g$. כלומר אם $f, g \in \mathcal{L}$ אז $\min(f, g) \in \mathcal{L}$.

מסקנה 13.22 אם $g \in \mathcal{L}$ אז קיימת סדרה $g_i \in \mathcal{L}$ ($i = 1, 2, \dots$) ו $g_i \nearrow g$ ולכל i קיימת $\varphi_i \in C_c^+(X)$ כך ש $g_i \le \varphi_i$.

הוכחה: לוקחים $f_n \in C_c^+(X)$ עם $f_n \nearrow 1$ ו $g_n = \min(g, nf_n)$) ■

מראים שאם $g \in X \le 1$ אז $1 - g \in \mathcal{L}$ ואם $f, g \in \mathcal{L}$ אז $f + g \in \mathcal{L}$.

<u>לסיום:</u> נסמן בΩ את אוסף התת־קבוצות $A \subseteq X$ כך ש $\mathrm{Char}_A \in \mathcal{L}$. אז Ω מכילה את כל הקבוצות הפתוחות, Ω סגורה לפעולת המשלים $(1 - g)$, Ω סגורה לחיתוך סופי ($\min(f, g)$) ולכן לאיחוד סופי, וΩ סגורה לאיחוד בן מנייה: תנאי 2 ומאיחוד סופי. לכן Ω מכילה את כל הקבוצות הבורל. כלומר: אם $A \in \mathcal{B}(X)$ אז $\mathrm{Char}_A \in \mathcal{L}$. מסיקים ש$\mathcal{L}$ מכילה כל פונקציה פשוטה $(f + g, af)$ ובעזרת קירוב מונוטוני $f_n \nearrow f$ מסיקים שf מכילה כל פונקציה מדידה בורל $f : X \to [0, \infty]$. ■

13.4 רגולריות

(מבוסס על Rudin)

הגדרה 13.23 מידת בורל μ על מרחב טופולוגי X נקראת רגולרית אם:

1. $K \subseteq X$ קומפקטית $\Longleftarrow$ $\mu(K) < \infty$

2. אם $\mathcal{O}\subseteq X$ פתוחה, אז

$$\mu\left(\mathcal{O}\right) = \sup\left\{ \mu\left(K\right)\mid K\subseteq\mathcal{O}\mid K\text{ is compact}\right\}$$

3. אם $A\subseteq X$ בורל אז

$$\mu\left(A\right) = \inf\left\{ \mu\left(\mathcal{O}\right)\mid A\subseteq\mathcal{O}\mid\mathcal{O}\text{ is open in X}\right\}$$

הערה 13.24 (תכונה): אם μ מידת בורל רגולרית על X, אז μ נקבעת באופן יחיד על ידי ערכי $\int_{X}fd\mu$ כאשר $f\in C_{c}^{+}\left(X\right)$.

הוכחה: אכן, לפי 3, די להראות כי $\mu\left(\mathcal{O}\right)$ נקבעת באופן יחיד עבור $\mathcal{O}$ פתוחה, אבל לכל $K\subseteq\mathcal{O}$ קומפקטית יש $K\prec f\prec\mathcal{O}$ ואז

$$\mu\left(K\right) \leq \int_{X}fd\mu\leq\mu\left(\mathcal{O}\right)$$

ולכן לפי 2 נובע כי $\mu\left(\mathcal{O}\right)=\sup\left\{ \int_{X}fd\mu\mid f\prec\mathcal{O}\right\}$. ■

טענה 13.25 (Rudin, page 50, Theorem 2.18): אם X מרחב טופולוגי שבו כל קבוצה פתוחה היא σ־קומפקטית, אז כל מידת בורל μ על X המקיימת תנאי 1 היא רגולרית.

משפט 13.26 (Riesz): (ראה גם Rudin, page 42) יהי X מרחב טופולוגי האוסדורף קומפקטי מקומית. יהי $\Lambda:C_{c}\left(X\right)\to\mathbb{C}$ פונקציונל לינארי. אם Λ אי־שלילי, במובן של $f\in C_{c}^{+}\left(X\right)$ מתקיים $\Lambda\left(f\right)\geq0$, אז קיימת מידת בורל יחידה μ על X כך שלכל $f\in C_{c}\left(X\right)$ מתקיים

$$\Lambda\left(f\right) = \int_{X}fd\mu$$

13.5 לגבי השוואת מכפלת מידות בין מידות על σ־אלגבראות, לבין מידות על מרחבים קומפקטיים מקומית

(לצורך σ־אלגבראות, נניח כי המרחבים הם σ־סופיים)
(ראה גם Cohn: Measure theory, proposition 7.6.2, page 242)
אם X,Y מרחבי האוסדורף קומפקטיים מקומית בעלי בסיס בן מנייה לטופולוגיה אז $\mathcal{B}\left(X\right)\times\mathcal{B}\left(Y\right)=\mathcal{B}\left(X\times Y\right)$, ואם μ,ν מידות בורל רגולריות על X,Y אז $\mu\times\nu$ (שניתן להגדרה ביחס לσ־אלגברה σ־סופית) היא מידת בורל רגולרית על $X\times Y$.

מסקנה 13.27 $\mu\times\nu$ היא מידת בורל (היחידה) המתקבלת הפונקציונאל

$$\begin{aligned}C_{c}\left(X\right)\otimes C_{c}\left(Y\right) & \longrightarrow\mathbb{C}\\ f\otimes g & \mapsto\left[\int_{X}f\left(x\right)d\mu\left(x\right)\right]\left[\int_{Y}g\left(y\right)d\nu\left(y\right)\right]\end{aligned}$$

הוכחה: קיום נובע מהטענה לעיל. יחידות נובעת מכך שאם $F \in C_c(X \times Y)$, אז יש $K \subseteq X$ ו$K' \subseteq Y$ קומפקטיות כך ש $\mathrm{supp}F \subseteq K \times K'$ ואז F ניתנת לקירוב במ"ש ע"י פונקציות מהצורה

$$\sum_{i=1}^{n} f_i(x)\, g_i(y) \qquad {\scriptstyle \mathrm{supp} f_i \subseteq K \atop \mathrm{supp} g_i \subseteq K'}$$

(זה נובע ממשפט Stone-Weierstrass.) ■

הערה 13.28 לשדה מקומי יש בסיס בן־מנייה לטופולוגיה.

13.6 כפל מידה בפונקציה

יהי X קומפקטי מקומית. נניח שכל קבוצה פתוחה בX היא σ־קומפקטית. תהי μ מידת בורל רגולרית על X. תהי $\varphi : X \to [0,\infty)$ פונקציה רציפה. (או באופן כללי יותר, פונקציה מדידה שהינה גם חסומה על כל קבוצה קומפקטית?)

לכל $E \subseteq X$ נגדיר

$$\lambda(E) = \int_E \varphi(x)\, d\mu(x)$$

λ מידה (משפט ההתכנסות המונוטונית) וλ סופית על כל קבוצה קומפקטית, ולכן λ מידת בורל רגולרית על X.

לכל $f = \sum_{\text{finite}} a_i \mathrm{Char}_{A_i}$ פשוטה מתקיים

$$\begin{aligned}
\int_X f d\lambda &= \sum a_i \lambda(A_i) \\
&= \sum a_i \int \varphi(x)\, \mathrm{Char}_{A_i}(x)\, d\mu(x) \\
&= \int f(x)\, \varphi(x)\, d\mu(x)
\end{aligned}$$

מכאן מסיקים כי $\int_X f d\lambda = \int_X \varphi f d\mu$ לכל $f : X \to [0,\infty]$ מדידה. (ע"י קירוב $f_i \nearrow f$ פשוטות). בפרט שוויון זה נכון ל $f \in C_c(X)$ ולכן λ היא המידה המתקבלת בעזרת משפט Riesz מהפונקציונל

$$C_c(X) \ni f \quad \mapsto \quad \int_X f \varphi d\mu$$

מסמנים $d\lambda = \varphi d\mu$.

13.7 מידת האר

הגדרה 13.29 חבורה טופולוגית G היא חבורה ומרחב טופולוגי כך שפעולות החבורה הן רציפות.

הערה 13.30 (תכונה): לכל $a\in G$, ההעתקה

$$\begin{aligned} a:G & \to G\\ x & \mapsto ax \end{aligned}$$

היא הומיאומורפיזם.

הגדרה 13.31 (סימון): אם μ מידת בורל רגולרית על G, נסמן מידה μ_a ע"י

$$\mu_a\left(E\right)=\mu\left(aE\right)\qquad\left(E\in\mathcal{B}\left(G\right)\right)$$

אזי μ_a מידת בורל רגולרית.

הגדרה 13.32 (סימון): לכל פונקציה f המוגדרת על G נסמן בf_a את הפונקציה על G הנתונה ע"י

$$f_a\left(x\right)=f\left(a^{-1}x\right)\qquad\left(x\in G\right)$$

הערה 13.33 (נוסחה): אם $f:G\to\left[0,\infty\right]$ מדידה ואם μ מידת בורל רגולרית על G, אז

$$\int f_a d\mu = \int f d\mu_a$$

הוכחה: ראשית אם $f=\mathrm{Char}_E$ (כאשר $E\in\mathcal{B}\left(G\right)$) אז

$$\begin{aligned} \left(\mathrm{Char}_E\right)_a\left(x\right) & = \begin{cases} 1 & a^{-1}x\in E\\ 0 & a^{-1}x\notin E \end{cases}\\ & = \begin{cases} 1 & x\in aE\\ 0 & x\notin aE \end{cases}\\ & = \left(\mathrm{Char}_{aE}\right)\left(x\right) \end{aligned}$$

כלומר $\left(\mathrm{Char}_E\right)_a=\mathrm{Char}_{aE}$. מכאן

$$\begin{aligned} \int\left(\mathrm{Char}_E\right)_a d\mu & = \int\mathrm{Char}_{aE}d\mu\\ & = \mu\left(aE\right)\\ & = \mu_a\left(E\right)\\ & = \int\mathrm{Char}_E d\mu_a \end{aligned}$$

וע"י צירופים לינאריים וגבולות, מקבלים את הנוסחה במקרה הכללי. ■

משפט 13.34 (מידת האר): (ראה גם Hewitt-Ross-Abstract Harmonic Analysis Vol-ume I (15,5) page 185 וגם (15,7) page 195)

תהי G חבורה טופולוגית האוסדורף קומפקטית מקומית, אז קיים פונקציונל לינארי $0 \neq I : C_c(G) \to \mathbb{C}$ כך ש I אי־שלילי במובן ש $I(f) \geq 0$ לכל $f \in C_c^+(G)$ וכך ש I אינווריאנטי משמאל במובן ש $I(f_a) = I(f)$ לכל $f \in C_c(G)$ וכמו כן, I נקבע באופן יחיד עד כדי סקלר חיובי. (ראה גם Weil)

הערה 13.35 (יישום משפט Riesz): תהי $\mu_G = \mu$ המידה בורל רגולרית המתאימה לI. אז לכל $f \in C_c(G)$ ולכל $a \in G$ מתקיים

$$\begin{aligned}\int f d\mu &= I(f) \\ &= I(f_a) \\ &= \int f_a d\mu \\ &= \int f d\mu_a\end{aligned}$$

מאחר וμ וμ_a רגולריות, נובע כי $\mu = \mu_a$, כלומר

$$\mu(aE) = \mu(E) \qquad (E \in \mathcal{B}(G))$$

וμ נקבעת באופן יחיד עד כדי סקלר חיובי ע"י תנאי זה. (זאת היות וμ מידת בורל רגולרית)

לבסוף, השוויון $\int_G f_a d\mu = \int_G f d\mu$ מתקיים לכל $f : G \to [0, \infty]$ בורל. (בעזרת פונקציות פשוטות וקירוב מונוטוני)

הערה 13.36 (תכונות):

1. אם $\emptyset \neq \mathcal{O} \subseteq G$ פתוחה אז $\mu(\mathcal{O}) > 0$. (אחרת ניתן לכסות כל קבוצה קומפקטית ע"י מספר סופי של הזזות של $\mathcal{O}$ ולהפוך את המידה להיות 0)
2. G קומפקטית $\iff \mu(G) < \infty$

הוכחה: $\Longleftarrow$: מיידי מרגולריות.

$\Longrightarrow$: נניח שG לא קומפקטית ונוכיח $\mu(G) = \infty$. אכן, תהי U סביבה פתוחה של 1_G עם $\overline{U}$ קומפקטית, ותהי V סביבה פתוחה של 1_G עם $VV^{-1} \subseteq U$. בעזרת רקורסיה ניתן לבנות סדרה $x_1, x_2, \ldots$ כך ש $x_{n+1} \notin \bigcup_{i=1}^n x_i U$ (לכל n טבעי) (הסבר: אם $G = \bigcup_{i=1}^n x_i U$ אז נובע שG קומפקטית ־ סתירה)

עבור $i < j$ נקבל ש $x_j \notin x_i U = x_i VV^{-1}$ כלומר $(x_j V) \cap (x_i V) = \emptyset$ ולכן $\{x_i V\}_{i=1}^\infty$ זרות בזוגות ופתוחות ו

$$\mu(x_i V) = \mu(V) > 0 \qquad (\forall i)$$

ולכן $\mu(G) = \infty$. ■

3. G דיסקרטית $\iff$ $\mu(\{x\})>0$ ל $x\in G$ כלשהו, ובמקרה זה μ פרופורציונית למידה הסופרת.

הוכחה: $\Longleftarrow$: נובע מ1 כי כל נקודה היא קבוצה פתוחה.

$\Longrightarrow$: תהי U סביבה פתוחה של 1_G כך ש $\overline{U}$ קומפקטית. אז $\mu\left(\overline{U}\right)<\infty$ ולכן $\overline{U}$ סופית. בפרט U סופית ופתוחה, ואז

$$\{1_G\} = U\setminus \underbrace{\{x\in U \mid x\neq 1_G\}}_{\text{finite set and therefore closed}}$$

פתוחה. מכאן שG דיסקרטית, והחלק האחרון מיידי. ■

4. אם G_1,G_2 חבורות טופולוגיות, האוסדורף, קומפקטיות מקומית וσ־קומפקטיות אז

$$\mu_{G_1\times G_2} = \mu_{G_1}\times\mu_{G_2}$$

מידת האר על $G_1\times G_2$.

5. אם $C_c^+(G)\ni f\neq 0$ אז $\int f d\mu>0$ כי יש $G\supseteq\mathcal{O}\neq\emptyset$ ו $c>0$ כך ש $f\geq c\cdot\mathrm{Char}_{\mathcal{O}}$.

6. אם $H\leq G$ תת־חבורה פתוחה, אז צמצום מידת האר של G על H היא מידת האר על H.

13.8 תת־חבורות נורמליות סגורות

תהי G חבורה טופולוגית האוסדורף קומפקטית מקומית. תהי $H\triangleleft G$ תת־חבורה נורמלית סגורה. אז G/H חבורה טופולגית (עם טופולוגיית המנה).

הגדרה 13.37 (סימון): נסמן איבר ב G/H ע"י $\dot{g}$ ואז $\dot{g}\in G/H$ כאשר g מסמן נציג כלשהו של $\dot{g}$: $\dot{g}=gH$.

תהי $f\in C_c(G)$. אז לכל $g\in G$, הפונקציה

$$\begin{array}{ccc} H & \to & \mathbb{C} \\ h & \mapsto & f(gh) \end{array}$$

שייכת ל$C_c(H)$.

(ראה גם Gaal - Linear Analysis and Representation Theory page 261, proposition 5)

לכן אם נסמן ב μ_H את מידת האר משמאל של H, מוגדר

$$\int_H f(gh)\,d_Hh = \int_H f(gh)\,d\mu_H(h)$$

ולכל $h_1\in H$ מתקיים

$$\int_H f(gh_1h)\,d_Hh = \int_H f(g(h_1h))\,d_Hh = \int_H f(gh)\,d_Hh$$

לכן ניתן להגדיר פונקציה

$$\begin{aligned} F : G/H &\to \mathbb{C} \\ F(g) &= \int_H f(gh)\, d_H h \end{aligned}$$

ו $F \in C_c(G/H)$ (ראה שוב בGaal).

מסקנה 13.38 מוגדר פונקציונל

$$\begin{aligned} I : C_c(G) &\to \mathbb{C} \\ I(f) &= \int_{G/H} \left[\int_H f(gh)\, d_H h \right] d_{G/H} \dot{g} \end{aligned}$$

כאן $d_{G/H}\dot{g} = d\mu_{G/H}\dot{g}$ ו$\mu_{G/H}$ מידת האר משמאל על G/H.
לכל $a \in G$ מתקיים:

$$\begin{aligned} I(f_a) &= \int_{G/H} \left[\int_H f_a(gh)\, d_H h \right] d_{G/H} \dot{g} \\ &= \int_{G/H} \left[\int_H f\left(a^{-1}gh\right) d_H h \right] d_{G/H} \dot{g} \end{aligned}$$

כעת

$$F_{\dot{a}}(\dot{g}) = F\left(\overbrace{a^{-1}\dot{g}}^{\cdot}\right) = F\left(\overbrace{a^{-1}g}^{\cdot}\right) = \int_H f\left(a^{-1}gh\right) d_H h$$

ולכן

$$\begin{aligned} I(f_a) &= \int_{G/H} \left[\int_H f\left(a^{-1}gh\right) d_H h \right] d_{G/H} \dot{g} \\ &= \int_{G/H} F_{\dot{a}}(\dot{g})\, d_{G/H} \dot{g} \\ &= \int_{G/H} F(\dot{g})\, d_{G/H} \dot{g} \\ &= \int_{G/H} \left[\int_H f(gh)\, d_H h \right] d_{G/H} \dot{g} \end{aligned}$$

ברור ש $I \geq 0$. נבדוק ש $I \neq 0$: אכן, אם נקח $0 \neq f \in C_c^+(G)$ אז קיים $g \in G$ כך שהפונקציה

$$\begin{aligned} H &\to \mathbb{C} \\ h &\to f(gh) \end{aligned}$$

אינה אפס ולכן $0 \neq F \in C_c^+(G/H)$, ואז $I(F) > 0$.

לכן I פונקציונל האר על G וקיימת מידת האר μ_G כך שלכל $f\in C_c(G)$ מתקיים:

$$\int_G f(x)\,d\mu_G(x) = \int_{G/H}\left[\int_H f(gh)\,d_H h\right] d_{G/H}\dot{g}$$

הערה 13.39 ניתן לקבוע כל שתיים מבין המידות האר μ_H, $\mu_{G/H}$, μ_G, ואז השלישית נקבע אוטומטית כך שהשוויון

$$\int_G f(x)\,d\mu_G(x) = \int_{G/H}\left[\int_H f(gh)\,d_H h\right] d_{G/H}\dot{g}$$

נכון.

טענה 13.40 תהי $f:G\to[0,\infty]$ מדידה בורל. נניח שכל קבוצה פתוחה בG היא σ־קומפקטית. אז לכל $g\in G$, הפונקציה

$$\begin{aligned} H &\to [0,\infty] \\ h &\mapsto f(gh) \end{aligned}$$

מדידה בורל על H (מיידי) והפונקציה $F:G/H\to[0,\infty]$ הנתונה ע"י $F(g)=\int_H f(gh)\,d_H h$ מוגדרת (מיידי) ומדידה בורל ולבסוף

$$\int_G f(x)\,d\mu_G(x) = \int_{G/H}\left[\int_H f(gh)\,d_H h\right] d_{G/H}\dot{g}$$

מתקיים.

הוכחה: נסמן ב$\mathcal{L}$ את אוסף הפונקציות המקיימות את הטענה. אז צריך לבדוק

1. $C_c^+(G)\subseteq\mathcal{L}$ (כבר ראינו)
2. אם $0\le f_1\le f_2\le\ldots$ ו $f_i\in\mathcal{L}$ לכל i, אז $f:=\lim_{i\to\infty}f_i\in\mathcal{L}$. (זאת מסקנה ממשפט ההתכנסות המונוטונית)
3. אם $f_i\in\mathcal{L}$ (לכל i) וקיימת $\varphi\in C_c^+(G)$ כך ש

$$0\le\ldots\le f_2\le f_1\le\varphi$$

אז $f:=\lim_{i\to\infty}f_i\in\mathcal{L}$.

נבדוק את 3: $\varphi-f_i$ מוגדרת על G.

$$\begin{aligned} 0 &\le \int(\varphi-f_i)(gh)\,d_H(h) \\ &= \int\varphi(gh)\,d_H(h)-\int f_i(gh)\,d_H(h) \end{aligned}$$

$$\begin{aligned}\int_G (\varphi - f_i) &= \int_G \varphi - \int_G f_i \\ &= \int_{G/H} \left[\int \varphi(gh)\, dh\right] d\dot{g} - \int_{G/H} \left[\int f_i(gh)\, dh\right] d\dot{g}\end{aligned}$$

אבל $\int_G (\varphi - f_i)$ מונוטוני שואף ל $\int_G (\varphi - f) = \int_G \varphi - \int_G f$ ואילו הביטוי $\int_{G/H} \left[\int \varphi(gh)\, dh\right] d\dot{g} - \int_{G/H} \left[\int f_i(gh)\, dh\right] d\dot{g}$ מונוטוני שואף ל $\int_{G/H} \left[\int \varphi(gh)\, dh\right] d\dot{g} - \int_{G/H} \left[\int f(gh)\, dh\right] d\dot{g}$ ומהנתון $\int_{G/H} \left[\int \varphi(gh)\, dh\right] d\dot{g} = \int_G \varphi$ ולכן קיבלנו

$$\int_G f = \int_{G/H} \left[\int f(gh)\, dh\right] d\dot{g}$$

■

13.9 תת־חבורות דיסקרטיות ותחומים יסודיים

הגדרה 13.41 תהי G חבורה טופולוגית האוסדורף, קומפקטית מקומית. $H \leq G$ תת־חבורה. H נקראת דיסקרטית אם הטופולוגיה מושרית מG על H דיסקרטית.

הערה 13.42 (תכונה): אם $H \leq G$ דיסקרטית, אז H סגורה.

הוכחה: יש סביבה פתוחה $U \subseteq G$ של 1_G כך ש $H \cap U = \{1_G\}$. תהי $V^{-1} = V \subseteq G$ סביבה פתוחה של 1_G בG כך ש $VV^{-1} = V^2 \subseteq U$.

יהי $x \in \overline{H}$. אז קיים $h \in (xV) \cap H$. מתקיים $(xV) \cap H = \{h\}$, כי אם $h' \in (xV) \cap H$ אז יש $v, v' \in V$ כך ש $h = xv$ ו $h' = xv'$ ואז $x = hv^{-1} = h'(v')^{-1}$ ולכן $H \ni (h')^{-1} h = (v')^{-1} v \in V^{-1}V = V^2 \subseteq U$. מאחר ש $H \cap U = \{1_G\}$, נובע ש $1_G = (h')^{-1} h$ ומכאן $h' = h$.

הוכחנו: $xV \cap H = \{h\}$. אם $h \neq x$ אז $xV \setminus \{h\}$ קבוצה פתוחה המכילה את x ואינה חותכת את H. בסתירה לכך ש $x \in \overline{H}$, ולכן $x = h \in H$. ■

תהי $H \lhd G$ תת־חבורה דיסקרטית נורמלית. נתייחס למידה הסופרת על H. נקבל שלכל פונקציה מדידה

$$f : G \to [0, \infty]$$

מתקיים

$$\int_G f(x)\, d_G x = \int_{G/H} \left[\sum_{h \in H} f(gh)\right] d_{G/H}\dot{g}$$

כאשר $d_G = d\mu_G$ ו $d_{G/H} = d\mu_{G/H}$ ו$\mu_{G/H}$, μ_G הן מידות האר משמאל הקובעות אחת את השנייה.

הגדרה 13.43 תהי G חבורה טופולוגית קומפקטית מקומית. $H \triangleleft G$ תת־חבורה נורמלית דיסקרטית. תחום יסודי $D \subseteq G$ היא תת־קבוצה בורל כך שלכל $g \in G$, הקבוצה $(gH) \cap D$ מכילה בדיוק איבר אחד. כלומר D מכילה נציג יחיד של כל קוסט.

במצב זה העתקת המנה

$$\begin{aligned} q_D = q\restriction_D : D & \rightarrow G/H \\ g & \mapsto gH \end{aligned}$$

חד־חד־ערכית ועל ורציפה, ולכן לכל $A \subseteq G/H$ בורל, $(q_D)^{-1}(A) \subseteq D$ בורל.

כעת תהי $\varphi : G/H \to [0,\infty]$ בורל, אז $\varphi \circ q = \varphi \circ q_D : D \to [0,\infty]$ בורל. נגדיר $f : G \to [0,\infty]$ ע"י

$$f(g) = \begin{cases} \varphi(q(g)) & g \in D \\ 0 & g \notin D \end{cases}$$

אז f בורל ו

$$\begin{aligned} \int_D (\varphi \circ q)(x)\, d_G x &= \int_G f(x)\, d_G x \\ &= \int_{G/H} \left[\sum_{h \in H} f(gh)\right] d_{G/H}\dot{g} \\ &= \int_{G/H} \varphi(\dot{g})\, d_{G/H}\dot{g} \end{aligned}$$

בפרט, אם נקח $\varphi = 1$ על G/H נקבל

$$\mu_{G/H}(G/H) = \int_{G/H} 1 d_{G/H}\dot{g} = \int_D 1 d_G x = \mu(D)$$

כלומר מידת התחום היסודי שווה למידת G/H (כאשר המידות מתואמות, כלומר $d\mu_G$ ו$d\mu_{G/H}$ מידות האר הקובעות אחת את השנייה)

13.9.1 קיום תחומים יסודיים

(באופן כללי זה נושא מסובך מאוד, אצלנו זה יהיה פשוט יחסית)

טענה 13.44 תהי G חבורה קומפקטית מקומית, σ־קומפקטית ו $H \triangleleft G$ תת־חבורה דיסקרטית נורמלית. אז קיים תחום יסודי.

הוכחה: תהי $V^{-1} = V \subseteq G$ סביבה פתוחה של 1_G כך ש $(V^{-1}V) \cap H = V^2 \cap H = \{1_G\}$. אז לכל $g \in G$ ההעתקה

$$\begin{aligned} q\restriction_{gV} : gV & \longrightarrow G/H \\ x & \mapsto xH \end{aligned}$$

חד־חד־ערכית (כי אם $gvH = gv'H$ אז $(v')^{-1} v \in H$ $V^{-1}V \ni$ ולכן $v = v'$).

קיימת סדרה $\{g_n\}_{n=1}^{\infty}$ כך ש $G=\bigcup_{n=1}^{\infty}g_nV$ (נובע מσ קומפקטיות). נגדיר

$$D = \bigcup_{n=1}^{\infty}\left(g_nV-\left(\bigcup_{k=1}^{n-1}g_kVH\right)\right)$$

אז

1. D בורל
2. $q(D)=G/H$ (כי לכל $g\in G$ יש n מינימלי כך ש $(g_nV)\cap(gV)\neq\emptyset$)
3. ההעתקה $q_D=q\restriction_D\colon D\to G/H$ היא חד־חד־ערכית: אכן, תהיינה $x,y\in D$ עם $q(x)=q(y)$. אז יש m,n כך ש $y\in g_mV-\left(\bigcup_{k=1}^{m-1}g_kVH\right)$, $x\in g_nV-\left(\bigcup_{k=1}^{n-1}g_kVH\right)$. אם $m<n$, אז נקבל סתירה כי $xH=yH$ ואז

$$x\in yH \quad\subseteq\quad g_mVH\subseteq\bigcup_{k=1}^{n-1}g_kVH$$

לכן $m=n$, מכאן $x,y\in g_nV$, אבל q חד־חד־ערכית על g_nV ולכן $x=y$.

■

13.10 מודולוס

תהי G חבורה טופולוגית האוסדורף קומפקטית מקומית. יהי $\sigma:G\to G$ אוטומורפיזם (אלגברי והומיאומורפיזם). תהי μ מידת האר משמאל (מימין) על G. נגדיר מידת בורל $\sigma^*\mu$ על G ע"י

$$(\sigma^*\mu)(A)=\mu\left(\sigma^{-1}(A)\right)\qquad(A\in\mathcal{B}(G))$$

אז $\sigma^*\mu$ מידת האר משמאל (מימין) על G. מיחידות מידת האר נובע שקיים מספר $\operatorname{mod}_G(\sigma)>0$ כך ש

$$\sigma^*\mu = (\operatorname{mod}_G(\sigma))^{-1}\mu$$

מכאן

$$\mu(\sigma(A))=\operatorname{mod}_G(\sigma)\mu(A)\qquad(A\in\mathcal{B}(G))$$

אכן,

$$\mu(A) = \mu\left(\sigma^{-1}(\sigma(A))\right)=(\sigma^*\mu)(\sigma(A))=(\operatorname{mod}_G\sigma)^{-1}\mu(\sigma(A))$$

כמו כן, לכל $f:G\to[0,\infty]$ מדידה

$$\begin{aligned}\int_G f(\sigma(x))\,d\mu(x) &= (\operatorname{mod}_G\sigma)^{-1}\int_G f(x)\,d\mu(x)\\ &= \text{"}\int_G f(x)\,d\mu\sigma^{-1}x\text{"}\end{aligned}$$

כדי לזכור, כלומר:

$$d\mu\left(\sigma^{-1}x\right) = \left(\mathrm{mod}_G\sigma\right)^{-1}d\mu\left(x\right)$$

או

$$d\mu\left(\sigma y\right) = \left(\mathrm{mod}_G\sigma\right)d\mu\left(y\right)$$

הוכחה: בעזרת קירוב מונוטוני די לבדוק עבור $f=\mathrm{Char}_A$ ($A\in\mathcal{B}\left(G\right)$) ואז

$$\begin{aligned}\mathrm{Char}_A\left(\sigma x\right) &= \begin{cases}1 & \sigma\left(x\right)\in A\\ 0 & \sigma\left(x\right)\notin A\end{cases}\\ &= \begin{cases}1 & x\in\sigma^{-1}\left(A\right)\\ 0 & x\notin\sigma^{-1}\left(A\right)\end{cases}\\ &= \mathrm{Char}_{\sigma^{-1}\left(A\right)}\left(x\right)\end{aligned}$$

ולכן

$$\begin{aligned}\int_G\mathrm{Char}_A\left(\sigma x\right)d\mu\left(x\right) &= \int_G\mathrm{Char}_{\sigma^{-1}A}\left(x\right)d\mu\left(x\right)\\ &= \mu\left(\sigma^{-1}\left(A\right)\right)\\ &= \left(\sigma^*\mu\right)\left(A\right)\\ &= \left(\mathrm{mod}_G\sigma\right)^{-1}\mu\left(A\right)\\ &= \left(\mathrm{mod}_G\sigma\right)^{-1}\int_G\mathrm{Char}_A\left(x\right)d\mu\left(x\right)\end{aligned}$$

■

הערה 13.45

1. $\mathrm{mod}_G\left(\sigma_1\sigma_2\right)=\mathrm{mod}_G\left(\sigma_1\right)\cdot\mathrm{mod}_G\left(\sigma_2\right)$
2. אם G קומפקטית אז $\mathrm{mod}_G\sigma=1$ לכל σ, כי $\sigma\left(G\right)=G$ ו $0<\mu\left(G\right)<\infty$ ואז

$$\left(0,\infty\right)\ni\mu\left(G\right) = \mu\left(\sigma\left(G\right)\right)=\left(\mathrm{mod}_G\sigma\right)\mu\left(G\right)$$

3. אם G דיסקרטית אז $\mathrm{mod}_G\sigma=1$ (לוקחים $A=\left\{1_G\right\}$)
4. כרגע $\mathrm{mod}_G\sigma$ רק תלוי בבחירת הצד של μ ימין או שמאל וזאת לאור יחידות מידת האר.

הערה 13.46 (דוגמה): יהי K שדה טופולוגי האוסדורף קומפקטי מקומית לא דיסקרטי. (הערה: ב[Weil] מוכיחים שאלו בדיוק השדות המקומיים). אז $\left\langle K,+\right\rangle$ חבורה טופולוגית קומפקטית מקומית. לכל $a\in K^\times$ יש אוטומורפיזם $a\cdot:\left\langle K,+\right\rangle\to\left\langle K,+\right\rangle$ ע"י $x\mapsto ax$. מכאן נקבל מספר $\mathrm{mod}\left(a\right)=\mathrm{mod}_{\left\langle K,+\right\rangle}a>0$ כך ש $\mu\left(aE\right)=\mathrm{mod}\left(a\right)\mu\left(E\right)$. עבור $a=0$ נסמן $\mathrm{mod}0=0$ והתכונה לעיל נשמרת.

הערה 13.47 (דוגמה): תהי G חבורה טופולוגית האוסדורף קומפקטית מקומית. לכל $g\in G$ יש אוטומורפיזם הצמדה $C_g:G\to G$ המוגדר ע"י $x\mapsto gxg^{-1}$.

הגדרה 13.48 המודולוס של G הוא הפונקציה

$$\begin{aligned}\delta:G &\to (0,\infty)\\ g &\mapsto \delta(g)=\mathrm{mod}_G(C_G)\end{aligned}$$

אז $\mu\left(gAg^{-1}\right)=\delta(g)\mu(A)$ (לכל $A\in\mathcal{B}(G)$).

הגדרה 13.49 אם $\delta(g)=1$ לכל $g\in G$ אז G נקראת אונימודולרית.

הערה 13.50 (תכונות):

1. אם G קומפקטית או דיסקרטית או חילופית, אז G מודולרית.
2. $\delta:G\to(0,\infty)$ הומומורפיזם רציף.

הוכחה: תכונת ההומומורפיזם מיידית. נבדוק רציפות: תהי U סביבה פתוחה של 1_G עם $\overline{U}$ קומפקטי. אז $0<\mu\left(\overline{U}\right)<\infty$. ע"י נרמול μ, נניח כי $\mu\left(\overline{U}\right)=1$. יהי $\varepsilon>0$. תהי $\overline{U}\subseteq W\subseteq G$ קבוצה פתוחה עם $\mu(W)<1+\varepsilon$. לכל $x\in\overline{W}$ יש סביבה פתוחה $1_G\in V_x=V_x^{-1}$ כך ש

$$V_x\cdot x\cdot V_x^2 \subseteq W$$

יש כיסוי סופי $\overline{U}\subseteq\bigcup_{i=1}^n x_iV_{x_i}$. נסמן $V=\bigcap_{i=1}^n V_{x_i}$. אז $V=V^{-1}$ ומתקיים $g\overline{U}g^{-1}\subseteq W$ לכל $g\in V$ (כי לכל $i=1,\ldots,n$ מתקיים $g\left(x_iV_{x_i}\right)g^{-1}\subseteq V_{x_i}x_iV_{x_i}^2\subseteq W$)

מכאן נובע כי לכל $g\in V$

$$\delta(g) = \delta(g)\cdot 1=\delta(g)\mu\left(\overline{U}\right)=\mu\left(C_g\left(\overline{U}\right)\right)=\mu\left(g\overline{U}g^{-1}\right)\leq\mu(W)<1+\varepsilon$$

וכמו כן, מתקיים גם $g\in V^{-1}\implies g^{-1}\in V$ ו $\delta(g)^{-1}=\delta\left(g^{-1}\right)<1+\varepsilon$.
כלומר $\frac{1}{1+\varepsilon}<\delta(g)<1+\varepsilon$ לכל $g\in V$ ולכן δ רציפה. ■

3. אינטגרציה:

$$\begin{aligned}\int_G f\left(gxg^{-1}\right)d\mu(x) &= \delta(g)^{-1}\int_G f(x)\,d\mu(x)\\ &= \int_G f(x)\,d\mu\left(g^{-1}xg\right)\end{aligned}$$

כלומר

$$d\left(g^{-1}xg\right) = d\left(C_g^{-1}(x)\right)=\left(\mathrm{mod}_G C_G\right)^{-1}dx$$

או

$$d\mu\left(gxg^{-1}\right) = \delta(g)\,d\mu(x)$$

למידת האר משמאל:

$$\int_G f\left(xg^{-1}\right)d\mu\left(x\right) = \int_G f\left(gxg^{-1}\right)d\mu\left(x\right)=\delta\left(g\right)^{-1}\int_G f\left(x\right)d\mu\left(x\right)$$

כלומר

$$\begin{aligned} d\mu\left(xg^{-1}\right) &= \delta\left(g\right)d\mu\left(x\right)\\ \mu\left(Ag^{-1}\right) &= \delta\left(g\right)\mu\left(A\right)\end{aligned}$$

למידת האר מימין:

$$\begin{aligned}\int_G f\left(gx\right)d\mu\left(x\right) &= \int_G f\left(gxg^{-1}\right)d\mu\left(x\right)=\delta\left(g\right)^{-1}\int_G f\left(x\right)d\mu\left(x\right)\\ d\mu\left(gx\right) &= \delta\left(g\right)d\mu\left(x\right)\\ \mu\left(gA\right) &= \delta\left(g\right)\mu\left(A\right)\end{aligned}$$

בGaal: $\Delta\left(g\right)=\delta\left(g\right)^{-1}$.

טענה 13.51 (תכונה): יהי $\sigma:G\to G$ אוטומורפיזם (טופולוגי), אז

$$\delta\left(\sigma\left(g\right)\right) = \delta\left(g\right)$$

לכל $g\in G$.

הוכחה: בספר Invariance of structure. ■

13.11 מעבר בין מידות האר משמאל ומימין

טענה 13.52 תהי G חבורה טופולוגית האוסדורף קומפקטית מקומית. $\delta:G\to\left(0,\infty\right)$ פונקציית המודולוס (כרגע ביחס למידת האר משמאל). תהי μ_l מידת האר משמאל. אז $\mu_r:=\delta\cdot\mu_l$ היא מידת האר מימין.

הוכחה: ברור ש $0\neq\mu_r\geq0$ וכמו כן μ_r מידה רגולרית (הוכחנו זאת אם כל קבוצה פתוחה היא σ-קומפקטית, ונראה שזה נכון באופן כללי). נותר לבדוק אינווריאנטיות מימין.
תהי $f\in C_c^+\left(G\right)$. מתקיים

$$\begin{aligned}\int_G f\left(xg\right)d\mu_r\left(x\right) &= \int_G f\left(xg\right)\delta\left(x\right)d\mu_l\left(x\right)\\ &= \delta\left(g\right)^{-1}\left[\int_G f\left(xg\right)\delta\left(xg\right)d\mu_l\left(x\right)\right]\\ &= \delta\left(g\right)^{-1}\left[\int_G f\left(y\right)\delta\left(y\right)d\mu_l\left(yg^{-1}\right)\right]\\ &= \delta\left(g\right)^{-1}\left[\delta\left(g\right)\int_G f\left(y\right)\delta\left(y\right)d\mu_l\left(y\right)\right]\\ &= \int_G f\left(y\right)d\mu_r\left(y\right)\end{aligned}$$

■

מסקנה 13.53 יהי $\sigma : G \to G$ אוטומורפיזם של G. אז $\mathrm{mod}_G(\sigma)$ זהה ביחס למידות האר מימין ומשמאל.

הוכחה: תהי μ_l מידת האר משמאל, δ הפונקציה המודולרית הנבנית עפ"י μ_l. נסמן $\mu_r = \delta\mu_l$ את מידת האר מימין. יהי $(\mathrm{mod}_G(\sigma))_l$ המודולוס כפי שנבנה לפי μ_l. נבדוק פעולת σ על אינטגרציה ביחס ל μ_r: תהי $f \in C_c^+(G)$

$$\begin{aligned}\int_G f(\sigma(x))\, d\mu_r(x) &= \int_G f(\sigma(x))\,\delta(x)\, d\mu_l(x)\\ &= \int_G f(\sigma(x))\,\delta(\sigma(x))\, d\mu_l(x)\\ &= (\mathrm{mod}_G\sigma)_l^{-1}\int f(x)\,\delta(x)\, d\mu_l(x)\\ &= (\mathrm{mod}_G\sigma)_l^{-1}\int f(x)\, d\mu_r(x)\end{aligned}$$

ולכן $(\mathrm{mod}_G\sigma)_r = (\mathrm{mod}_G\sigma)_l$. ■

מסקנה 13.54 G אונימודולרית $\iff$ אוסף מידות האר מימין ומשמאל זהה.

הוכחה: $\Longleftarrow$: מיידי (כי $\mu_r = \delta\mu_l$)

$\Longrightarrow$: מניחים שכל מידת האר μ היא גם מימין וגם משמאל ולכל A בורל ו $g \in G$ מתקיים

$$\delta(g)\,\mu(A) = \mu\left(gAg^{-1}\right) = \mu(A)$$

■

מסקנה 13.55 (פונקציית ההופכי): תהי μ_l מידת האר משמאל על G. נגדיר $\check{\mu}_l(A) = \mu_l\left(A^{-1}\right)$ (לכל $A \in \mathcal{B}(G)$). אז ברור ש$\check{\mu}_l$ מידת האר מימין. ו

$$\int_G f\left(x^{-1}\right) d\mu_l(x) = \int_G f(x)\, d\check{\mu}_l(x)$$

לכן קיים $c > 0$ כך ש $\check{\mu}_l = c \cdot \delta\mu_l$. מתקיים $c = 1$, כלומר $\check{\mu}_l = \delta\mu_l$ ולכן לכל $f : G \to (0,\infty)$ מתקיים

$$\int_G f\left(x^{-1}\right) d\mu_l(x) = \int_G f(x)\,\delta(x)\, d\mu_l(x)$$

הוכחה: (ש$c = 1$): יהי $\varepsilon > 0$. תהי $V = V^{-1}$ סביבה פתוחה של 1_G עם $\overline{V}$ קומפקטית.

ואז $0<\mu_l(V)<\infty$) וכך ש $1-\varepsilon<\delta(g)<1+\varepsilon$ (לכל $g\in V$). אז

$$\begin{aligned}\mu_l(V) &= \mu_l\left(V^{-1}\right)\\ &= \check{\mu}_l(V)\\ &= \int_G \mathrm{Char}_V(x)\,d\check{\mu}_l(x)\\ &= \int_G c\cdot\mathrm{Char}_V(x)\,\delta(x)\,d\mu_l(x)\\ &= c\int_V \delta(x)\,d\mu_l(x)\in c\mu_l(V)\left[1-\varepsilon,1+\varepsilon\right]\end{aligned}$$

זה נכון לכל $\varepsilon>0$ ולכן $c=1$. ■

13.12 חבורת מנה

למה 13.56 (Weil, page 3): תהי G חבורה טופולוגית האוסדורף קומפקטית מקומית, $G'\triangleleft G$ תת חבורה נורמלית סגורה. נסמן $G''=G/G'$. יהי λ אוטומורפיזם (טופולוגי) על G כך ש $\lambda(G')=G'$. אז λ משרה אוטומורפיזם (טופולוגי) על G' ו־G'' (מסומנים גם ב־λ) ומתקיים

$$\mathrm{mod}_G(\lambda) = \mathrm{mod}_{G'}(\lambda)\cdot\mathrm{mod}_{G''}(\lambda)$$

הוכחה: תהיינה α,α',α'' מידות האר משמאל על G,G',G'' מתאומות. אז עבור $f\in C_c^+(G)$ מתקיים

$$\begin{aligned}\mathrm{mod}_G(\lambda)\int_G f(x)\,d\alpha(x) &= \int_G f\left(\lambda^{-1}(x)\right)d\alpha(x)\\ &= \int_{G''}\left[\int_{G'} f\left(\lambda^{-1}(gz)\right)d\alpha'(z)\right]d\alpha''(\dot{g})\\ &= \int_{G''}\left[\int_{G'} f\left(\lambda^{-1}(g)\,\lambda^{-1}(z)\right)d\alpha'(z)\right]d\alpha''(\dot{g})\\ &= \mathrm{mod}_{G'}(\lambda)\int_{G''}\left[\int_{G'} f\left(\lambda^{-1}(g)\,z\right)d\alpha'(z)\right]d\alpha''(\dot{g})\end{aligned}$$

נסמן

$$F(\dot{g}) = \int_{G'} f(gz)\,d\alpha'(z)$$

אז

$$\begin{aligned}
\operatorname{mod}_G(\lambda)\int_G f(x)\,d\alpha(x) &= \operatorname{mod}_{G'}(\lambda)\int_{G''}\left[\int_{G'} f\left(\lambda^{-1}(g)\,z\right)d\alpha'(z)\right]d\alpha''(\dot g)\\
&= \operatorname{mod}_{G'}(\lambda)\int_{G''}\left[F\left(\lambda^{-1}(\dot g)\right)\right]d\alpha''(\dot g)\\
&= \operatorname{mod}_{G'}(\lambda)\cdot\operatorname{mod}_{G''}(\lambda)\cdot\int_{G''}F(\dot g)\,d\alpha''(\dot g)\\
&= \operatorname{mod}_{G'}(\lambda)\cdot\operatorname{mod}_{G''}(\lambda)\cdot\int_{G''}\left[\int_{G'} f(gz)\,d\alpha'(z)\right]d\alpha''(\dot g)\\
&= \operatorname{mod}_{G'}(\lambda)\cdot\operatorname{mod}_{G''}(\lambda)\cdot\int_G f(x)\,d\alpha(x)
\end{aligned}$$

■

13.13 פרספקטיבה על קבוצת נציגים ומרחבים פולנים

מבוסס על [Cohn, Measure theory, chapter 8]

הגדרה 13.57 מרחב פולני הוא מרחב טופולוגי עם תת־קבוצה בת־מנייה צפופה וכן שקיימת מטריקה שלמה המשרה את הטופולוגיה.

הערה 13.58 (דוגמה): מרחב טופולוגי האוסדורף קומפקטי מקומית עם בסיס בן מניה לטופולוגיה הוא מרחב פולני (ראה עמוד 255 בספר הנ"ל).

משפט 13.59 (מיון של תת־קבוצות בורל של מרחבים פולנים): יהי X מרחב פולני ו $A\in\mathcal{B}(X)$. אז המרחב המדיד $\langle A,\mathcal{B}(A)\rangle$ איזומורפי ל $\langle E,\mathcal{B}(E)\rangle$ כאשר E אחד מהמרחבים הטופולוגיים הבאים:

- קבוצה ריקה
- קבוצה סופית
- קבוצה בת־מניה עם הטופולוגיה הדיסקרטית
- $[0,1]$ עם הטופולוגיה הרגילה

מסקנה 13.60 (עמוד 215): שני מרחבים מדידים סטנדרטיים (כמו במשפט) איזומורפיים אם ורק אם יש להם אותה עוצמה וזאת יכולה להיות רק 0, סופית, בת־מניה או הרצף.

משפט 13.61 (על מדידת פונקציות הפוכות) (ראה גם עמוד 274, 276): תהי A תת־קבוצת בורל של מרחב פולני, ויהי Y מרחב פולני. תהי $S:\langle A,\mathcal{B}(A)\rangle\to\langle Y,\mathcal{B}(Y)\rangle$ פונקציה מדידה וחד־חד־ערכית אז

1. $S(A)\subseteq Y$ בורל
2. $S:A\to S(A)$ איזומורפיזם בורל

משפט 13.62 (על קיום חתך) (ראה עמוד 287, תרגיל 4) (זה לא בדיוק תרגיל, זה משפט די רציני): יהי X מרחב פולני ויהי (Y,Σ) מרחב מדיד. תהי $q:X\to Y$ כך ש

1. לכל $y\in Y$ מתקיים כי $q^{-1}(y)\subseteq X$ סגורה לא ריקה (בפרט q על)
2. אם $U\subseteq X$ פתוחה אז $q(U)\in\Sigma$.

אז קיימת $s:Y\to X$ מדידה ביחס ל$\mathcal{B}(X)$ וΣ כך ש $q\circ s=\mathrm{id}_Y$.

מסקנה 13.63 תהי G חבורה טופולוגית האוסדורף קומפקטית מקומית עם בסיס בן מניה לטופולוגיה. תהי $H\subseteq G$ תת־חבורה סגורה. אז G/H מרחב האוסדורף קומפקטי מקומית עם בסיס בן מנייה לטופולוגיה. לכן G וG/H מרחב פולנים. ההטלה $q:G\to G/H$ המוגדרת ע"י $g\mapsto gH$ מקיימת תנאים 1+2 לעיל, ולכן קיימת $s:G/H\to G$ מדידה עם $q\circ s=\mathrm{id}_{G/H}$. בפרט s חד־חד־ערכית. לכן אם נסמן $D=s(G/H)$ נקבל בעזרת המשפט על מדידות הפונקציה ההפוכה ש

1. $D\subseteq G$ בורל
2. $s:G/H\to D$ איזומורפיזם בורל

לכן D תחום יסודי עבור H, ולבסוף $q\restriction_D: D\to G/H$ איזומורפיזם בורלי (כי הוא שווה להופכי של s בסעיף 2).

14 טרנספורם פוריה על שדה מקומי

14.1 פונקציית מודולוס

יהי K שדה מקומי לא ארכימדי (עם מציין 0). π ראשוני.

$$\mathcal{O} \quad = \quad \{x\mid |x|\leq 1\}$$

חוג השלמים, $\mathcal{P}=\pi\mathcal{O}$ האידאל המקסימלי. תהי μ מידת האר על $\langle K,+\rangle$. $\mathcal{O}$ פתוחה וקומפקטית ולכן $0<\mu(\mathcal{O})<\infty$.

נניח כי $\mu(\mathcal{O})=1$. לכל $a\in K^{\times}$ מוגדר

$$\mathrm{mod}a \quad = \quad \frac{\mu(a\mathcal{O})}{\mu(\mathcal{O})}$$

לכן אם $a\in\mathcal{O}^{\times}$ נובע ש $\mathrm{mod}a=1$. נמצא את $\mathrm{mod}\pi$. נסמן:

$$q \quad = \quad \#\overline{K}=\#(\mathcal{O}/\mathcal{P})=\#(\mathcal{O}/\pi\mathcal{O})$$

תהי $0\in S\subseteq\mathcal{O}$ קבוצת נציגים ל $\overline{K}=\mathcal{O}/\pi\mathcal{O}$. אז $\#S=q$. יש איחוד זר $\mathcal{O}=\bigcup_{s\in S}(s+\pi\mathcal{O})$ ו $\mu(s_1+\pi\mathcal{O})=\mu(s_2+\pi\mathcal{O})$ (כאשר $s_1,s_2\in S$) ולכן נקבל

$$\mu(s+\pi\mathcal{O}) \quad = \quad \frac{1}{q}$$

לכל $s\in S$. בפרט $\mu\left(\pi\mathcal{O}\right)=\frac{1}{q}$ ומכאן

$$\text{mod}\pi = \frac{\mu\left(a\mathcal{O}\right)}{\mu\left(\mathcal{O}\right)}=\frac{1}{q}$$

ע"י החלפת ההערכה $|\cdot|$ ב $|\cdot|^{\rho}$ (נירמול), אפשר להניח כי $|\pi|=\frac{1}{q}$ ואז נובע כי $\text{mod}\left(a\right)=|a|$ לכל $a\in K$, ואז אומרים ש$|\cdot|$ מנורמלת.

הערה 14.1 עבור $\mathbb{Q}_p$ מתקיים $p=\#\overline{\mathbb{Q}_p}=q$ ולכן $|\cdot|_p$ מנורמלת. ($|p|_p=\frac{1}{p}$)

הערה 14.2 (נוסחאות):

$$\begin{aligned}\mu\left(aE\right) &= |a|\,\mu\left(E\right)\\ \int_K f\left(a^{-1}x\right)dx &= \int_K f\left(x\right)d\left(ax\right)=|a|\int_K f\left(x\right)dx\\ d\left(ax\right) &= |a|\,dx\end{aligned}$$

(כאשר $dx=d\mu\left(x\right)$)

14.2 שדות מקומיים

טענה 14.3 יהי K שדה מקומי לא ארכימדי עם מציין 0. אז K הרחבה סופית של $\mathbb{Q}_p$ עבור p מתאים.

הערה 14.4

1. $p=\text{char}\overline{K}$
2. $K\supseteq\mathbb{Q}_p$ הוא הסגור של $K\supseteq\mathbb{Q}$

הוכחה: $K\supseteq\mathbb{Q}$. תהי $|\cdot|$ ההערכה של K. ראשית הצמצום של $|\cdot|$ על $\mathbb{Q}$ לא טריוואלי. אחרת $|x|=1$ לכל $x\in\mathbb{Q}$ ומכאן $|x-y|=1$ לכל $x,y\in\mathbb{Q}$ ובפרט

$$\mathbb{Q} \subseteq \mathcal{O}=\{z\in K \mid |z|\le 1\}$$

ו$\mathcal{O}$ מרחב מטרי קומפקטי עם סדרת נקודות בעלות מרחק 1 ביניהן. סתירה. (לסדרת נקודות כנ"ל אין תת־סדרה מתכנסת)

לכן יש ראשוני p כך שהצמצום של $|\cdot|$ על $\mathbb{Q}$ שקול ל$|\cdot|_p$. ע"י החלפת $|\cdot|$ ב $|\cdot|^{\rho}$ אפשר להניח ש $|\cdot|$ מצומצמת ל$\mathbb{Q}$ הוא $|\cdot|_p$. K שלם ולכן $\overline{\mathbb{Q}}=\mathbb{Q}_p\subseteq K$. נותר להוכיח ש $\dim_{\mathbb{Q}_p}\left(K\right)<\infty$. נוכיח זאת בדרך השלילה: נניח כי המימד הנ"ל $=\infty$. יהי $0\neq a\in\mathbb{Q}$ עם $|a|<1$ (למשל $a=p$). נסתכל על האוטומורפיזם $\lambda=a\cdot:K\to K$ המוגדר ע"י $x\mapsto ax$, השומר את $\mathbb{Q}$ וλ הוא $\mathbb{Q}_p$־לינארי. לכל n טבעי קיים תת־מרחב וקטורי $V\subseteq K$ עם $\dim_{\mathbb{Q}_p}V=n$. K מרחב נורמי מעל $\mathbb{Q}_p$. לכן V מרחב נורמי מעל $\mathbb{Q}_p$ עם מימד סופי. מכאן $V\subseteq K$ סגור, וכמו כן יש איזומורפיזם של מרחבים וקטוריים טופולוגיים:

$$V \cong \mathbb{Q}_p^n$$

(הנורמות שקולות). לכן

$$\mathrm{mod}_V\left(a\cdot\right) \quad = \quad \left|a\right|_p^n = \left|a\right|^n$$

ראינו שמתקיים

$$0 < \mathrm{mod}_K a \quad = \quad \left(\mathrm{mod}_V a\right)\left(\mathrm{mod}_{K/V} a\right) = \left|a\right|^n\left(\mathrm{mod}_{K/V} a\right)$$

נבדוק בהמשך ש $\mathrm{mod}_{K/V} a \leq 1$ ונסיק ש $0 < \mathrm{mod}_K a \leq \left|a\right|^n$ לכל $n = 1, 2, \ldots$. אבל $\left|a\right| < 1$ ולכן נקבל סתירה.

$\mathrm{mod}_{K/V} a \leq 1$: מאחר ש $\left|a\right| < 1$ שנובע ש $a\cdot\mathcal{O} \subseteq \mathcal{O}$. תהי $\eta : K \to K/N$ ההטלה. אז $a\eta\left(\mathcal{O}\right) \subseteq \eta\left(\mathcal{O}\right)$ ב K/V. אבל $\eta\left(\mathcal{O}\right) \subseteq K/V$ פתוחה וקומפקטית ולכן מידת האר שלה לפי K/V סופית וחיובית. לכן $\mathrm{mod}_{K/V} a \leq 1$. ■

14.3 בניית קרקטר חיבורי (רציף)

14.3.1 $\mathbb{Q}_p$

<u>הנוסחה:</u> לכל $x \in \mathbb{Q}_p$ יש תיאור

$$x \quad = \quad \frac{a_{-k}}{p^k} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + \ldots$$

עם $a_i \in \{0, 1, \ldots, p-1\}$ (לכל i). נסמן את החלקי השברי

$$\{x\} \quad = \quad \frac{a_{-k}}{p^k} + \cdots + \frac{a_{-1}}{p}$$

ונגדיר $e_p : \mathbb{Q}_p \to \mathbb{C}$ ע"י

$$\begin{aligned} e_p\left(x\right) &= \exp\left(-2\pi i\left\{x\right\}\right) \\ &= \exp\left(-2\pi i\left(\frac{a_{-k}}{p^k} + \cdots + \frac{a_{-1}}{p}\right)\right) \\ &= e^{-2\pi i\left(\frac{a_{-k}}{p^k} + \cdots + \frac{a_{-1}}{p}\right)} \end{aligned}$$

הערה 14.5 (תכונות):

1. $x \in \mathbb{Z}_p \iff e_p\left(x\right) = 1$
2. $e_p\left(x+y\right) = e_p\left(x\right)\cdot e_p\left(y\right)$

בפרט e_p קרקטר רציף של $\mathbb{Q}_p$.

תיאור אחר: $\{x\}$ מספר רציונלי מהצורה $\frac{n}{p^j}$ כך ש $x \in \{x\} + \mathbb{Z}_p$, ואז $\{x\}$ נקבע מודולו $\mathbb{Z}$. צריך לבדוק ש $\frac{n}{p^j} \in \mathbb{Z}_p$ אם ורק אם $\frac{n}{p^j} \in \mathbb{Z}$ (שלם). ואכן נניח ש $\gcd\left(n, p\right) = 1$ ואז

$$\left|\frac{n}{p^j}\right| \quad = \quad p^j$$

קטן או שווה ל1 אם ורק $j \leq 0$.

14.3.2 קרקטרים על שדה מקומי K (לא ארכימדי)

הגדרה 14.6 קרקטר χ של חבורה G (כלומר הומומורפיזם $\chi : G \to \mathbb{C}^{\times}$) נקרא אוניטרי אם $\chi(G) \subseteq \mathbb{T}$, באשר $\mathbb{T} = \{z \mid |z| = 1\}$ מעגל היחידה.

הערה 14.7 יהי $\chi : K \to \mathbb{C}^{\times}$ קרקטר (תמיד נניח כי הוא רציף). אז לכל n יש צמצום $\chi : P^n \to \mathbb{C}^{\times}$ ו־P^n קומפקטית, ולכן $\chi(P^n)$ תת־חבורה קומפקטית של $\mathbb{C}^{\times}$ ולכן $\chi(P^n) \subseteq \mathbb{T}$.

מסקנה 14.8 χ אוניטרי.

ראינו שאם K שדה מקומי לא ארכימדי עם מציין 0, אז $K/\mathbb{Q}_p$ הרחבה סופית ויש העתקת עקבה $\mathrm{Tr} : K \to \mathbb{Q}_p$ והיא על (כי היא אינה אפס ו־$\mathbb{Q}_p$־לינארית). מתקיים גם $|\mathrm{Tr}(x)| \leq |x|$. אכן, אם $\mathbb{Q}_p \subseteq K \subseteq L$ הרחבת גלואה של $\mathbb{Q}_p$ המכילה את K, אז יש צמודים $x_1, \ldots, x_n \in L$ של x מעל $\mathbb{Q}_p$ כך ש $\mathrm{Tr}x = \sum_{i=1}^{n} x_i$, ומאחר ש־$x_i$ צמוד לx, ראינו ש $|x| = |x_i|$ ולכן $|\mathrm{Tr}x| \leq \max_{i=1}^{n} |x_i| = |x|$. בפרט $\mathrm{Tr}\mathcal{O} \subseteq \mathbb{Z}_p$. (כאשר $\mathcal{O} = \{x \in K \mid |x| \leq 1\}$ חוג השלמים של K)

נגדיר $\chi = e_p \circ \mathrm{Tr} : K \to \mathbb{C}^{\times}$ כלומר $\chi(x) = e^{-2\pi i \{\mathrm{Tr}(x)\}}$. אז χ קרקטר, רציפות נובעת מכך ש $\chi(\mathcal{O}) = 1$. כמו כן $\chi \neq 1$ כי Tr על ו $e_p \neq 1$.

14.3.3 מוביל (Conductor) של קרקטר

π ראשוני, $P^n = \pi^n \mathcal{O}$. יהי $\chi : K \to \mathbb{C}^{\times}$ קרקטר לא טריוואלי רציף. קיים n שלם כך ש $\chi(P^n) \subseteq \left\{z \in \mathbb{C}^{\times} \mid |z-1| < \frac{1}{2}\right\}$. מאחר ש $\chi(P^n) \subseteq \mathbb{T}$ תת־חבורה, נובע ש $\chi(P^n) = 1$. מאחר ש $\chi \neq 1$, קיים n שלם כך ש

$$\begin{aligned} \chi \restriction_{P^{n-1}} &\neq 1 \\ \chi \restriction_{P^n} &= 1 \end{aligned}$$

P^n נקרא המוביל של χ.

הערה 14.9 (דוגמה): המוביל של e_p על $\mathbb{Q}_p$ הוא $\mathbb{Z}_p$ כי $e_p(\mathbb{Z}_p) = 1$ ו $e_p\left(\frac{1}{p}\right) = e^{-\frac{2\pi i}{p}} \neq 1$.

כעת בסימונים לעיל, נסתכל על הקרקטר χ' הנתון ע"י

$$\chi'(x) = \chi(\pi^n x) \qquad (x \in K)$$

אז $\chi'(\mathcal{O}) = 1$ ו

$$\chi'\left(P^{-1}\right) = \chi'\left(\pi^{-1}\mathcal{O}\right) = \chi\left(\pi^{n-1}\mathcal{O}\right) = \chi\left(P^{n-1}\right) \neq 1$$

ולכן המוביל של χ' הוא $\mathcal{O}$.

הערה 14.10 לכל $a \in K$ מגדירים קרקטר $\chi_a : K \to \mathbb{C}^{\times}$ ע"י

$$\chi_a(x) = \chi(ax) \qquad (x \in K)$$

14.4 פונקציית שוורץ

K שדה מקומי לא ארכימדי (ממציין 0?).

הגדרה 14.11 פונקציה $f:K\to\mathbb{C}$ נקראת שוורץ אם:

1. f קבועה מקומית (כלומר לכל $x\in K$ יש סביבה $x\in V_x\subseteq K$ כך ש $f\restriction_{V_x}$ קבועה)
2. $\mathrm{supp}f:=\{x\in K\mid f(x)\neq 0\}$ קומפקטי.

הערה 14.12 אם 1 אז נובע ש$\mathrm{supp}f$ המוגדר ב2 אוטומטית קבוצה סגורה.

הגדרה 14.13 (סימון): נסמן את אוסף פונקציות שוורץ ב $\mathcal{S}(K)$.

טענה 14.14 (תיאור): לכל $f\in\mathcal{S}(K)$ יש תיאור מהצורה

$$f = \sum_{i=1}^{l} c_i \mathrm{Char}_{\alpha_i+P^n}$$

כאשר $n\in\mathbb{Z}$, $\alpha_i\in K$, $c_i\in\mathbb{C}$ ו $\{\alpha_i+P^n\}_{i=1}^{l}$ זרות.

הוכחה: יש שוויון מהצורה

$$\mathrm{supp}f = \bigcup_{i=1}^{m}\left(a_i+P^{n_{a_i}}\right)$$

כאשר $n_{a_i}\in\mathbb{Z}$ וf קבועה על $a_i+P^{n_{a_i}}$ (כי f פונקציה קבועה מקומית ו $\mathrm{supp}f$ קומפקטית).
נסמן $n=\max_{i=1}^{l} n_{a_i}$ ונקבל שsupp איחוד (זר) של קוסטים מהצורה $a+P^n$. מכאן התיאור.
■

14.5 טרנספורם פוריה

יהי $\chi:K\to\mathbb{C}^\times$ קרקטר עם מוביל $\mathcal{O}$.

הגדרה 14.15 תהי $f:K\to\mathbb{C}$ פונקציית שוורץ. אז טרנספורם פוריה של f הינו פונקציה $\hat{f}:K\to\mathbb{C}$ הנתונה ע"י

$$\hat{f}(y) = \int_K f(x)\chi(-xy)\,dx$$

הערה 14.16 באופן מדויק, $\hat{f}$ צריכה להיות פונקציה של הקרקטר $\varphi=\chi(\cdot y)$ כלומר

$$\hat{f}(\varphi)(y) = \int_K f(x)\varphi(-xy)\,dx$$

הערה 14.17 $dx=d\mu\left(x\right)$ כאשר μ מידת האר המקיימת $\mu\left(\mathcal{O}\right)=1$.

למה 14.18 תהי G טופולוגית האוסדורף קומפקטית ו $\chi:G\to\mathbb{C}^{\times}$ קרקטר (רציף) <u>לא טריוואלי</u> $(\chi\neq1)$. אז

$$\int_{G}\chi\left(g\right)dg\quad=\quad0$$

הוכחה: יהי $g_{0}\in G$ עם $\chi\left(g_{0}\right)\neq1$ אז

$$\int_{G}\chi\left(g\right)dg\quad=\quad\int_{G}\chi\left(g_{0}g\right)dg=\chi\left(g_{0}\right)\int_{G}\chi\left(g\right)dg$$

■

מסקנה 14.19 נסמן $\mathcal{S}\left(K\right)\ni\varphi_{0}=\mathrm{Char}_{\mathcal{O}}$, אזי $\widehat{\varphi_{0}}=\varphi_{0}$.

הוכחה: (בדיקה): אם $y\in\mathcal{O}$ אז $xy\in\mathcal{O}$ לכל $x\in\mathcal{O}$ ולכן

$$\begin{aligned}\widehat{\varphi_{0}}\left(y\right) & = \int_{K}\mathrm{Char}_{\mathcal{O}}\left(x\right)\chi\left(-xy\right)dx\\ & = \int_{\mathcal{O}}\chi\left(-xy\right)dx\\ & = \int_{\mathcal{O}}1dx\\ & = \mu\left(\mathcal{O}\right)=1\end{aligned}$$

נניח כי $y\notin\mathcal{O}$. אז יש $n<0$ כך $y\mathcal{O}=\mathcal{P}^{n}$. לכן הקרקטר

$$\begin{aligned}\chi\left(\cdot y\right)\restriction_{\mathcal{O}}:\mathcal{O} & \to \mathbb{C}^{\times}\\ x & \mapsto \chi\left(-xy\right)\end{aligned}$$

אינו טריוואלי (כי $\mathcal{O}$ הוא המוביל של χ). לכן מהלמה

$$\widehat{\varphi_{0}}\left(y\right)\quad=\quad\int_{\mathcal{O}}\chi\left(-xy\right)dx=0=\varphi_{0}\left(y\right)$$

■

הזזות ושינוי סקלה: תהי $f:K\to\mathbb{C}$ ויהיו $a\in K,b\in K^{\times}$. נסמן

$$f_{a,b}\left(x\right)=f\left(a+bx\right)\qquad\left(x\in K\right)$$

תכונות:

1. אם $f \in \mathcal{S}(K)$ אז $f_{a,b} \in \mathcal{S}(K)$
2. לאור התיאור של $\mathcal{S}(K)$ בסעיף הקודם, נובע שכל $f \in \mathcal{S}$ הוא צירוף לינארי של פונקציות מהצורה $(\varphi_0)_{a,b}$.

הערה 14.20 לכל $c \in K$, הפונקציה χ_c היא קבועה מקומית ו $\chi_0 = 1$.

חישוב: אם $f \in \mathcal{S}(K)$ אז לכל $c \in K$, $b \in K$, $a \in K$ מתקיים כי הפונקציה $\chi_c f_{a,b} \in \mathcal{S}(K)$ ומתקיים

$$\widehat{\chi_c f_{a,b}} = \underbrace{|b|^{-1}\chi\left(-\frac{ac}{b}\right)}_{\text{Number}} \cdot \underbrace{\chi_{\frac{a}{b}}}_{\text{Character}} \cdot \left(\hat{f}\right)_{-\frac{c}{b},\frac{1}{b}}$$

אכן

$$\begin{aligned}
\widehat{\chi_c f_{a,b}}(y) &= \int_K \chi_c(x) f(a+bx)\chi(-xy)\,dx \\
&= \int_K f(a+bx)\chi(cx-xy)\,dx \\
&= \int_K f(a+bx)\chi((c-y)x)\,dx \\
\underbrace{}_{\substack{t=a+bx \\ dt=|b|dx}} &= \frac{1}{|b|}\int_K f(t)\chi\left((c-y)\frac{t-a}{b}\right)dt \\
&= \frac{1}{|b|}\chi\left(-\frac{ca}{b}\right)\chi\left(y\frac{a}{b}\right)\int_K f(t)\chi\left((c-y)\frac{t}{b}\right)dt \\
&= \frac{1}{|b|}\chi\left(-\frac{ca}{b}\right)\chi\left(y\frac{a}{b}\right)\int_K f(t)\chi\left(-\frac{(y-c)}{b}t\right)dt \\
&= \frac{1}{|b|}\chi\left(-\frac{ca}{b}\right)\chi_{\frac{a}{b}}(y)\hat{f}\left(\frac{y-c}{b}\right) \\
&= \frac{1}{|b|}\chi\left(-\frac{ac}{b}\right)\chi_{\frac{a}{b}}(y)\hat{f}_{-\frac{c}{b},\frac{1}{b}}
\end{aligned}$$

טענה 14.21 אם $f \in S(K)$, אז $\hat{f} \in S(K)$ ומתקיים $\hat{\hat{f}}(x) = f(-x)$ לכל $x \in K$.

הוכחה: אפשר להניח $f = (\varphi_0)_{a,b}$ (כי $\mathcal{S}(K)$ צירוף לינארי של כאלה). מהנוסחה עם $c = 0$ נובע

$$\begin{aligned}
\widehat{(\varphi_0)_{a,b}} &= |b|^{-1}\cdot\chi_{\frac{a}{b}}\cdot(\widehat{\varphi_0})_{0,\frac{1}{b}} \\
&= |b|^{-1}\cdot\chi_{\frac{a}{b}}\cdot(\varphi_0)_{0,\frac{1}{b}}
\end{aligned}$$

וזוהי פונקציית שוורץ. לבסוף נשתמש שוב בנוסחה (עם $b=\frac{1}{b}$, $c=\frac{a}{b}$, $a=0$) ונקבל

$$\begin{aligned}\widehat{\widehat{(\varphi_0)_{a,b}}} &= |b|^{-1}\cdot\widehat{\chi_{\frac{a}{b}}\cdot(\varphi_0)_{0,\frac{1}{b}}}\\ &= |b|^{-1}\cdot\left|\frac{1}{b}\right|^{-1}\cdot\left(\widehat{\varphi_0}\right)_{-\frac{\frac{a}{b}}{\frac{1}{b}},\frac{1}{\frac{1}{b}}}\\ &= (\varphi_0)_{-a,b}\end{aligned}$$

לבסוף, חישוב ישיר מראה ש

$$(\varphi_0)_{-a,b}(x) = (\varphi_0)_{a,b}(-x)$$

משתמשים בכך ש $\varphi_0(x)=\varphi_0(-x)$ ואז

$$(\varphi_0)_{-a,b}(x) = \varphi(-a+bx)=\varphi(a-bx)=\varphi(a+b(-x))=\varphi_{a,b}(-x)$$

$\blacksquare$

הערה 14.22 (תבנית סימטרית): בכל מרחב מידה $\langle X,\Sigma,\mu\rangle$ השיקוף

$$\begin{aligned}X\times X &\longrightarrow X\times X\\ (x_1,x_2) &\mapsto (x_2,x_1)\end{aligned}$$

הוא אוטומורפיזם של $(X\times X,\Sigma\times\Sigma,\mu\times\mu)$. לכל y, התבנית

$$\begin{aligned}\mathcal{S}(K)\times\mathcal{S}(K) &\longrightarrow \mathbb{C}\\ (f,h) &\mapsto \int_K f(x)\,\hat{h}(xy)\,dx\end{aligned}$$

היא סימטרית. אכן, מתחילים מהתבנית

$$(f,h) \mapsto \int_{K^2} f(x)\,h(z)\,\chi(-xyz)\,dzdx$$

שהיא סימטרית, ולפי פוביני מתקיים

$$\begin{aligned}\int_{K^2} f(x)\,h(z)\,\chi(-xyz)\,dzdx &= \int_K f(x)\left[\int_K h(z)\,\chi(-xyz)\,dz\right]dx\\ &= \int_K f(x)\,\hat{h}(xy)\,dx\end{aligned}$$

קרקטרים יהי K שדה מקומי, ויהי $\chi:K\to\mathbb{C}^\times$ קרקטר לא טריוואלי עם מוביל $\mathcal{O}$.

טענה 14.23 לכל קרקטר $\eta:K\to\mathbb{C}^\times$ (רציף) קיים $a\in K$ יחיד כך ש $\eta=\chi_a$ (כלומר $\eta(x)=\chi(ax)$ לכל $x\in K$)

הוכחה: יהי $a\in K^{\times}$. נפרק $a=\pi^{l}u$ (כאשר $u\in\mathcal{O}^{\times}$). אז

$$a\in P^{n}\iff\chi_{a}\restriction_{P^{-n}}=1$$

(וזה נכון גם אם $a=0$)

$$\begin{array}{rcl}\chi_{a}\restriction_{P^{-n}}=1 & \iff & 1=\chi\left(aP^{-n}\right)=\chi\left(a\pi^{-n}\mathcal{O}\right)=\chi\left(\pi^{l}\pi^{-n}\mathcal{O}\right)=\chi\left(P^{l-n}\right)\\ & \iff & \\ P^{l-n}\subseteq\mathcal{O} & \iff & l\geq n\iff a\in P^{n}\end{array}$$

מכאן נובעת יחידות a (יחד עם $\chi_{a_1}\cdot\chi_{a_2}=\chi_{a_1+a_2}$, $\chi_{a}^{-1}=\chi_{-a}$): אם $\chi_{a_1}=\chi_{a_2}$ אז $\chi_{a_1-a_2}=1$ ובפרט $\chi_{a_1-a_2}\restriction_{P^{-n}}=1$ לכל n ולכן $a_1-a_2\in P^{n}$ לכל n ומכאן $|a_1-a_2|\leq|\pi|^{n}$ לכל n, ומכאן $|a_1-a_2|=0$.

נוכיח בהמשך שלכל $n=1,2,\ldots$ קיים $a_n\in K$ כך ש $\chi_{a_n}\restriction_{P^{-n}}=\eta\restriction_{P^{-n}}$, אז

$$\chi_{a_{n+1}}\restriction_{P^{-n}}=\chi_{a_{n+1}}\restriction_{P^{-(n+1)}}\restriction_{P^{-n}}=\mu\restriction_{P^{-n}}=\chi_{a_n}\restriction_{P^{-n}}$$

ולכן $\chi_{a_{n+1}-a_n}\restriction_{P^{-n}}=1$ ומכאן $a_{n+1}-a_n\in P^{n}$ כלומר $|a_{n+1}-a_n|\leq|\pi|^{n}$. לכן $\{a_n\}_{n=1}^{\infty}$ סדרת קושי וקיים $\lim_{n\to\infty}a_n=a$. יהי $x\in K$ ויהי $n_0\geq1$ כך ש $x\in P^{-n_0}$. לכל $n\geq n_0$ מתקיים $-n\leq-n_0$ ולכן $x\in P^{-n_0}\subseteq P^{-n}$ ומכאן

$$\eta\left(x\right)=\chi_{a_n}\left(x\right)=\chi\left(a_nx\right)$$

(לכל $n\geq n_0$). מרציפות χ נקבל

$$\chi_{a}\left(x\right)=\chi\left(ax\right)=\lim_{n\to\infty}\chi\left(a_nx\right)=\lim_{n\to\infty}\eta\left(x\right)=\eta\left(x\right)$$

כלומר $\chi_{a}=\eta$.

נותר להוכיח שלכל $n=1,2,\ldots$ קיים $a_n\in K$ כך ש $\chi_{a_n}\restriction_{P^{-n}}=\eta\restriction_{P^{-n}}$. לשם כך נגדיר פונקציה

$$\begin{array}{rcl}\mathcal{S}\left(K\right) & \ni & f:K\to\mathbb{C}\\ f & = & \left(\mathrm{Char}_{P^{-n}}\right)\cdot\eta\end{array}$$

ברור ש $f\neq0$ (כי $f\left(0\right)=1$). מאחר ש $\hat{\hat{f}}\left(x\right)=f\left(-x\right)$, מתקיים $\hat{f}\neq0$, ואז קיים $y\in K$ כך ש

$$0\neq\hat{f}\left(y\right)=\int_{K}f\left(x\right)\chi\left(-xy\right)dx=\int_{P^{-n}}\eta\left(x\right)\chi_{y}\left(-x\right)dx=\int_{P^{-n}}\left(\eta\cdot\chi_{y}^{-1}\right)dx$$

לבסוף, $\eta\cdot\chi_{y}^{-1}\restriction_{P^{n}}:P^{n}\to\mathbb{C}^{\times}$ זהו קרקטר של החבורה קומפקטית P^{-n}. אילו קרקטר זה היה לא טריוואלי, היינו מקבלים כי האינטגרל היה מתאפס. לכן $\eta\cdot\chi_{y}^{-1}\restriction_{P^{n}}$ טריוואלי, כלומר $\eta\restriction_{P^{n}}=\chi_{y}\restriction_{P^{n}}$ ונקח $y=a_n$. ∎

15 פונקציית זיטא ופונקציות L מקומיות

15.1 מידת האר על $K^{\times}$

K שדה מקומי, μ מידת האר על K (כך ש $\mu(\mathcal{O})=1$). נבדוק ש $\frac{dx}{|x|}=\frac{1}{|x|}d\mu(x)$ מידת האר על $K^{\times}$.

תהי $f:K^{\times}\to[0,\infty]$ מדידה. נגדיר (למשל) $f(0)=0$. אז לכל $a\in K^{\times}$

$$\begin{aligned}\int_{K^{\times}}f(ax)\frac{dx}{|x|} &= \int_{K}f(ax)\frac{1}{|x|}dx\\ &= \int_{K}f(ax)\frac{1}{|x|}\frac{d(ax)}{|a|}\\ &= \int_{K}f(x)\frac{d(x)}{|x|}\\ &= \int_{K^{\times}}f(x)\frac{d(x)}{|x|}\end{aligned}$$

נירמול: נסמן $q=\#\overline{K}=\#(\mathcal{O}/P)$ ויהי π ראשוני. ראינו ש:

$$\mu(P) = \mu(\pi\mathcal{O})=|\pi|\,\mu(\mathcal{O})=\frac{1}{q}$$

ולכן

$$\int_{\mathcal{O}^{\times}}\frac{dx}{|x|} = \int_{\mathcal{O}^{\times}}dx=\mu\left(\mathcal{O}^{\times}\right)=\mu(\mathcal{O}\setminus\mathcal{P})=1-q^{-1}$$

נסמן מידה מנורמלת

$$d^{\times}x = \frac{1}{1-q^{-1}}\frac{dx}{|x|}$$

זוהי מידת האר על $K^{\times}$ ו $\int_{\mathcal{O}^{\times}}d^{\times}x=1$.

15.2 קרקטרים על $K^{\times}$

יהי $\omega:K^{\times}\to\mathbb{C}^{\times}$ קרקטר (רציף). נסמן $U_0=\mathcal{O}^{\times}\subseteq K^{\times}$, $U_n=1+P^n\subseteq K^{\times}$ (כאשר $n=1,2,\ldots$). אז $\{U_n\}_{n=0}^{\infty}$ תתי־חבורות קומפקטיות פתוחות של $K^{\times}$ ומהוות בסיס לסביבות של 1. (U_n חבורה כי אם $x\in 1+P^n$ ל $n\geq 1$ אז $|x|=1$ ו $|x-1|\leq|\pi|^n$ ולכן $\left|1-x^{-1}\right|\leq|\pi|^n$).

מאחר שω רציף, קיים $n\geq 0$ כך ש

$$\omega(U_n) \subseteq \left\{z\in\mathbb{C}^{\times}\mid|z-1|<\frac{1}{2}\right\}$$

אז $\omega(U_n)$ חבורה ולכן $\omega(U_n)=1$.

הגדרה 15.1 אם $\omega\left(\mathcal{O}^{\times}\right)=1$ אז ω נקרא לא מסועף (Unramified).

הערה 15.2 במקרה זה, ω נקבע ע"י הערך $\omega\left(\pi\right)$: לכל $z\in K^{\times}$ יש פירוק יחיד $z=\pi^{n}u$ (כאשר $u\in\mathcal{O}^{\times}$) ואז

$$\omega\left(z\right) = \omega\left(\pi\right)^{n}=\omega\left(z\right)^{\mathrm{ord}_{K}z}$$

הגדרה 15.3 אם $\omega\left(\mathcal{O}^{\times}\right)\neq1$ אז ω נקרא מסועף

הערה 15.4 במקרה זה קיים $n\geq1$ כך ש $\omega\left(U_{n}\right)=1$ ו $\omega\left(U_{n-1}\right)\neq1$, כלומר $\omega\left(1+P^{n}\right)=1$ ו $\omega\left(1+P^{n-1}\right)\neq1$ (אם $n=1$, אז $\omega\left(\mathcal{O}^{\times}\right)\neq1$). P^{n} (כאשר $n\geq1$) נקרא המוביל של ω (ואם $n=0$ אומרים ש$\mathcal{O}^{\times}$ הוא המוביל)

הערה 15.5 אם ω חיובית, כלומר $\omega\left(x\right)>0$ (לכל $x\in K^{\times}$) אז $\omega\left(\mathcal{O}^{\times}\right)$ תת חבורה קומפקטית של $\left(0,\infty\right)$ (כי ω רציף ו $\mathcal{O}^{\times}$ קומפקטית), ולכן $\omega\left(\mathcal{O}^{\times}\right)=1$ וω לא מסועף. מאחר ש $\omega\left(\pi\right),\left|\pi\right|\in\left(0,\infty\right)$ ו$\left|\pi\right|\neq1$, קיים $s_{0}\in\mathbb{R}$ <u>יחיד</u> כך ש $\omega\left(\pi\right)=\left|\pi\right|^{s_{0}}$ ומכאן נובע

$$\left(x\in K^{\times}\right)\qquad\omega\left(x\right)=\left|x\right|^{s_{0}}$$

(כי אם $x\in\mathcal{O}^{\times}$, אז שני הצדדים 1)

כעת, יהי $\omega:K^{\times}\to\mathbb{C}^{\times}$ קרקטר (רציף) כלשהו. יש פירוק

$$\omega = \frac{\omega}{\left|\omega\right|}\cdot\left|\omega\right|$$

כאשר $\left|\omega\right|\left(x\right)=\left|\omega\left(x\right)\right|$ ($x\in K^{\times}$) ואז $\left|\omega\right|$ קרקטר חיובי ו $\frac{\omega}{\left|\omega\right|}$ קרקטר אוניטרי.

מסקנה 15.6 קיים קרקטר אוניטרי $\omega_{0}=\frac{\omega}{\left|\omega\right|}$ ומספר ממשי s_{0} כך ש

$$\omega = \omega_{0}\cdot\left|\cdot\right|^{s_{0}}$$

הערה 15.7 ראינו שניתן לקחת s_{0} ממשי ואז s_{0} יחיד. אם לוקחים $s_{0}\in\mathbb{C}$ אז כבר אין יחידות כי $\left|\cdot\right|^{it}$ גם קרקטר אוניטרי.

15.3 אינטגרל זיטא מקומי (K שדה מקומי לא ארכימדי עם מציין 0)

הגדרה 15.8 יהי $\omega:K^{\times}\to\mathbb{C}^{\times}$ קרקטר אוניטרי ו $f\in\mathcal{S}\left(K\right)$. עבור $s\in\mathbb{C}$ נגדיר (אם מתכנס):

$$Z\left(s,f,\omega\right) = \int_{K^{\times}}f\left(x\right)\omega\left(x\right)\left|x\right|^{s}d^{\times}x$$

ונסתכל על צד ימין כפונקציה של s.

הערה 15.9

1. מאחר ש

$$\left|K^{\times}\right| = \left\{|\pi|^{n}\right\}_{n=-\infty}^{\infty} = \left\{q^{n}\right\}_{n=-\infty}^{\infty}$$

כאשר $q = \#\overline{K}$, ומאחר ש

$$q^{s} = e^{s\log q}$$

נקבל ש $q^{\frac{2\pi i}{\log q}} = 1$ ולכן $|x|^{s} = |x|^{s+\frac{2\pi i}{\log q}}$ (לכל $x \in K^{\times}$) ולכן $s \mapsto Z(s,f,\omega)$ מחזורית עם מחזור $\frac{2\pi i}{\log q}$.

2. נקח $a = \pi$ או $a = \pi^{-1}$, אז $|a| = q$ או $|a| = q^{-1}$ ונחשב:

$$\begin{aligned} Z(s,\omega(a)f_{a},\omega) &= \int_{K^{\times}} \omega(a) f_{a}(x)\omega(x)|x|^{s} d^{\times}x \\ &= \frac{1}{|a|^{s}} \int_{K^{\times}} f(ax)\omega(ax)|ax|^{s} d^{\times}x \\ &= \frac{1}{|a|^{s}} \int_{K^{\times}} f(ax)\omega(ax)|ax|^{s} d^{\times}(ax) \\ &= q^{\pm s} Z(s,f,\omega) \end{aligned}$$

לכן אוסף הפונקציות $\{Z(s,f,\omega) \mid f \in \mathcal{S}(K)\}$ אינווריאנטי לכפל ב $q^{\pm s}$. (בכל תחום ההתכנסות)

15.4 התכנסות

יהי P^{n_0} המוביל של ω.

נניח ש$f(0) = 0$**.** אז לכל $a \in \operatorname{supp} f$ יש $n \geq n_0$ כך שf קבועה על $a(1+P^{n})$ וזוהי סביבה פתוחה של a (כי $a \neq 0$). מאחר ש $\operatorname{supp} f$ קומפקטי, יש $n \geq n_0$ כך שf צירוף לינארי של פונקציות מהצורה

$$\operatorname{Char}_{a(1+P^{n})} \qquad (a \neq 0)$$

נשתמש בפירוק

$$a = \pi^{\operatorname{ord}_{K} a} \cdot u \qquad \left(u \in \mathcal{O}^{\times}\right)$$

עבור $x \in a(1+P^{n})$ מתקיים

$$f(x)\omega(x)|x|^{s} = f(a)\omega(a)|a|^{s}$$

(כי f קבועה על $a(1+P^{n})$, $\omega = 1$ על $(1+P^{n})$ ו$|x| = |a|$ ל$x \in a(1+P^{n})$) ולכן

$$\begin{aligned} f(x)\omega(x)|x|^{s} &= f(a)\omega(a)|a|^{s} \\ &= f(a)\omega(a)\left(|\pi|^{\operatorname{ord}_{K} a}\right)^{s} \\ &= f(a)\omega(a) q^{-(\operatorname{ord}_{K} a)s} \end{aligned}$$

מסקנה 15.10 אם $f(0)=0$ אז לכל $s\in\mathbb{C}$ מתקיים כי Z פולינום ב$q^{\pm}$:

$$Z(s,f,\omega) = c_{-k}q^{-ks}+\cdots+c_0+\cdots+c_lq^{ls}$$

הערה 15.11 אם נקח $a=1$, אז $\mathrm{ord}_K a=0$ ואז נסיק כי שהפונקציה הקבועה 1 שייכת ל $\{Z(s,f,\omega)\mid f\in\mathcal{S}(K)\}$, ומהערה 2 נובע שכל פולינום ב $q^{\pm s}$ ניתן לקבל עם f מתאימה.

מקרה כללי תהי $f\in\mathcal{S}(K)$, אז יש פירוק יחיד

$$f = f(0)\,\mathrm{Char}_{\mathcal{O}}+f'$$

כאשר $f'(0)=0$. לכן די לבדוק את $f=f_0=\mathrm{Char}_{\mathcal{O}}$. נסמן $\sigma=\mathrm{Re}(s)$, אז

$$\begin{aligned}\int_{K^\times}\left|\mathrm{Char}_{\mathcal{O}}(x)\,\omega(x)\,|x|^s\right|d^\times x &= \int_{\mathcal{O}}|x|^\sigma\,d^\times x\\ &= \sum_{n=0}^{\infty}\int_{\pi^n\mathcal{O}}|x|^\sigma\,d^\times x\\ &= \sum_{n=0}^{\infty}|\pi|^{n\sigma}\\ &= \sum_{n=0}^{\infty}\frac{1}{q^{n\sigma}}=\frac{1}{1-\frac{1}{q^\sigma}}\end{aligned}$$

מתכנס אם $\sigma>0$.

מסקנה 15.12 $Z(s,f,\omega)$ מתכנס (בהחלט) כאשר $\mathrm{Re}s>0$.

15.5 תיאור אוסף הפונקציות $\{Z(s,f,\omega)\mid f\in\mathcal{S}(K)\}$

נסתכל על אוסף זה של פונקציות כפונקציות על $\mathrm{Re}s>0$. ראינו שאוסף זה נשמר ע"י כפל ב $q^{\pm s}$. אם נקח $f(0)=0$, נקבל את כל הפולינומים ב$q^{\pm s}$ המסומן ב $\mathbb{C}[q^s,q^{-s}]$. לכן די לבדוק שוב את הפונקציה $f=f_0=\mathrm{Char}_{\mathcal{O}}$.

$$\begin{aligned}Z(s,\mathrm{Char}_{\mathcal{O}},\omega) &= \int_{\mathcal{O}}\omega(x)\,|x|^s\,d^\times x\\ &= \sum_{n=0}^{\infty}\int_{\pi^n\mathcal{O}^\times}\omega(x)\,|x|^s\,d^\times x\end{aligned}$$

שראינו שמתכנס ל$0 < \mathrm{Re} s$. נציב $x = \pi^n y$, $d^\times x = d^\times y$. אז

$$\begin{aligned} &= \sum_{n=0}^{\infty} \int_{\mathcal{O}^\times} \omega\left(\pi^n y\right) \left|\pi^n y\right|^s d^\times x \\ &= \sum_{n=0}^{\infty} \omega\left(\pi^n\right) q^{-ns} \int_{\mathcal{O}^\times} \omega\left(y\right) \left|y\right|^s d^\times x \\ &= \begin{cases} 0 & \omega \text{ is ramified} \\ \sum_{n=0}^{\infty} \left(\omega\left(\pi\right) q^{-s}\right)^n = \frac{1}{1-\omega(\pi) q^{-s}} & \omega \text{ is unramified} \end{cases} \end{aligned}$$

כי במקרה המסועף $\omega \restriction_{\mathcal{O}^\times} \neq 1$ ולכן האינטגרל מתאפס, ואילו במקרה הלא מסועף $\omega \restriction_{\mathcal{O}^\times} = 1$.

מסקנה 15.13 לכל $f \in \mathcal{S}\left(K\right)$ יש המשכה מרומורפית ל $Z\left(s, f, \omega\right)$ על כל $\mathbb{C}$.

תיאור אוסף הפונקציות: מאחר ש

$$\frac{\mathbb{C}}{1-\omega\left(\pi\right) q^{-s}} + \mathbb{C}\left[q^s, q^{-s}\right] = \frac{\mathbb{C}\left[q^s, q^{-s}\right]}{1-\omega\left(\pi\right) q^{-s}}$$

נקבל ש

$$\left\{Z\left(s, f, \omega\right) \mid f \in \mathcal{S}\left(K\right)\right\} = \begin{cases} \mathbb{C}\left[q^s, q^{-s}\right] & \omega \text{ is ramified} \\ \frac{\mathbb{C}\left[q^s, q^{-s}\right]}{1-\omega(\pi) q^{-s}} & \omega \text{ is unramified} \end{cases}$$

מגדירים פונקציית L של ω ע"י

$$L\left(s, \omega\right) = \begin{cases} 1 & \omega \text{ is ramified} \\ \frac{1}{1-\omega(\pi) q^{-s}} & \omega \text{ is unramified} \end{cases}$$

ואז

$$\left\{Z\left(s, f\omega\right) \mid f \in \mathcal{S}\left(K\right)\right\} = \mathbb{C}\left[q^s, q^{-s}\right] \cdot L\left(s, \omega\right)$$

הערה 15.14 בדקנו שאם ω לא מסועף אז

$$Z\left(s, \mathrm{Char}_{\mathcal{O}}, \omega\right) = \frac{1}{1-\omega\left(\pi\right) q^{-s}} = L\left(s, \omega\right)$$

15.6 מקרה ארכימדי

יש הגדרות דומות אם השדה הוא $\mathbb{R}$ או $\mathbb{C}$. נתייחס ל$\mathbb{R}$.
קרקטר רציף $(0, \infty) \to \mathbb{C}^\times$ הוא מהצורה

$$t \mapsto t^{s_0} \qquad (t > 0)$$

אם $\omega : \mathbb{R}^\times \to \mathbb{C}^\times$ קרקטר, אז יש שתי אפשרויות:

1. $\omega\left(-1\right)=1$ (אז אומרים ש־ω לא מסועף)
2. $\omega\left(-1\right)=-1$ (אז אומרים ש־ω מסועף)

במקרה הראשון $\omega\left(t\right)=\left|t\right|^{s_0}$. במקרה שני $\omega\left(t\right)=\operatorname{sgn}\left(t\right)\cdot\left|t\right|^{s_0}$. לכן באינטגרל זיתא די להתייחס ל־$\omega=1$ או $\omega=\operatorname{sgn}$.

נתייחס ל־$\omega=1$, כמידת האר על $\mathbb{R}^{\times}$. נקח $d^{\times}x=\frac{dx}{|x|}$.

הנוסחה הכללית היא שוב:

$$Z\left(s,f,\omega\right) = \int_{\mathbb{R}^{\times}}f\left(x\right)\omega\left(x\right)\left|x\right|^{s}d^{\times}x=\int_{\mathbb{R}^{\times}}f\left(x\right)\omega\left(x\right)\left|x\right|^{s-1}dx$$

נקח $\omega=1$ ואז

$$Z\left(s,f,1\right) = \int_{\mathbb{R}^{\times}}f\left(x\right)\left|x\right|^{s}d^{\times}x$$

נקח $f\left(x\right)=e^{-\pi x^{2}}$:

$$\begin{aligned}Z\left(s,e^{-\pi x^{2}},1\right) & = \int_{\mathbb{R}^{\times}}e^{-\pi x^{2}}\left|x\right|^{s}d^{\times}x\\
 & = 2\int_{0}^{\infty}e^{-\pi x^{2}}x^{s-1}dx\\
 & = \frac{2}{2\pi}\int_{0}^{\infty}e^{-\pi x^{2}}x^{s-2}\left(2\pi x\right)dx\\
\underbrace{}_{\substack{u=\pi x^{2}\\ du=2\pi xdx\\ x=\left(\frac{u}{\pi}\right)^{\frac{1}{2}}}} & = \frac{1}{\pi}\int_{0}^{\infty}e^{-u}\left(\frac{u}{\pi}\right)^{\frac{s}{2}-1}du\\
 & = \pi^{-\frac{s}{2}}\int_{0}^{\infty}e^{-u}u^{\frac{s}{2}-1}du\\
 & = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\end{aligned}$$

בודקים שבעזרת $f\left(x\right)=\left(\underbrace{}_{\text{polynomial of x}}\right)\cdot e^{-\pi x^{2}}$ מקבלים $\left(\underbrace{}_{\text{polynomial of s}}\right)\cdot\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)$ (בודקים למונומים. עבור x^{2n+1} מדובר בפונקציה אי־זוגית, ולכן מקבלים 0. עבור x^{2n} יוצא ביטוי דומה למקרה הזה ומשתמשים בכך ש $\Gamma\left(\frac{2n+s}{2}\right)=\left(\frac{s}{2}+n-1\right)\left(\frac{s}{2}+n-2\right)\cdot\cdots\cdot\left(\frac{s}{2}+1\right)\cdot\Gamma\left(\frac{s}{2}\right)$).

לכן מסמנים $L_{\mathbb{R}}\left(s,1\right)=\pi^{-\frac{s}{2}}\cdot\Gamma\left(\frac{s}{2}\right)$. באופן דומה, מסמנים

$$L_{\mathbb{R}}\left(s,\operatorname{sgn}\right) = \pi^{-\left(\frac{s+1}{2}\right)}\Gamma\left(\frac{s+1}{2}\right)$$

(ראה גם Goldfeld-Hundley)

16 משוואה פונקציונאלית מקומית

16.1 הגדרת γ

K שדה מקומי, π ראשוני, μ מידת האר על K ו $\mu(\mathcal{O})=1$, χ קרקטר של K עם מוביל $\mathcal{O}$. הגדרנו טרנספורם פוריה

$$\hat{f}(y)=\int_K f(x)\chi(-xy)\,dx \qquad (f\in\mathcal{S}(K))$$

ω קרקטר כפלי אוניטרי. $d^\times x$ מידת האר על $K^\times$ עם $\int_{\mathcal{O}^\times}d^\times x=1$, $q=\#\overline{K}$. האינטגרל $Z(s,f,\omega)=\int_{K^\times}f(x)\omega(x)|x|^s\,d^\times x$ מתכנס בהחלט ובעל המשכה מרומורפית ל$\mathbb{C}$.

משפט 16.1 לכל $f,h\in\mathcal{S}(K)$ מתקיים

$$Z(s,f,\omega)Z\left(1-s,\hat{h},\omega^{-1}\right) = Z(s,h,\omega)Z\left(1-s,\hat{f},\omega^{-1}\right)$$

כאשר $0<\mathrm{Re}s<1$, ולכן לכל $\mathbb{C}$ ע"י המשכה אנליטית.

הוכחה: עבור $0<\mathrm{Re}s<1$ מתקיים

$$\begin{aligned}Z(s,f,\omega)Z\left(1-s,\hat{h},\omega^{-1}\right) &= \int_{K^\times}f(x)\omega(x)|x|^s\,d^\times x\cdot\int_{K^\times}\hat{h}(y)\omega^{-1}(y)|y|^{1-s}\,d^\times y\\ &= \int_{K^\times}\left(\int_{K^\times}f(x)\hat{h}(y)\omega\left(xy^{-1}\right)\left|xy^{-1}\right|^s|y|\,d^\times y\right)d^\times x\end{aligned}$$

נציב באינטגרל הפנימי $z=x^{-1}y$ (x קבוע), אז $d^\times y=d^\times z$ ו $xz=y$. נקבל

$$Z(s,f,\omega)Z\left(1-s,\hat{h},\omega^{-1}\right) = \int_{K^\times}\left(\int_{K^\times}f(x)\hat{h}(xz)\omega\left(z^{-1}\right)|z|^{-s}|xz|\,d^\times z\right)d^\times x$$

האינטגרל מתכנס בהחלט ולכן מפוביני ניתן להחליף את סדר האינטגרציה:

$$\begin{aligned}Z(s,f,\omega)Z\left(1-s,\hat{h},\omega^{-1}\right) &= \int_{K^\times}\left(\int_{K^\times}f(x)\hat{h}(xz)|x|\,d^\times x\right)\omega(z)^{-1}|z|^{1-s}\,d^\times z\\ &= \left(1-q^{-1}\right)^{-1}\int_{K^\times}\left(\int_K f(x)\hat{h}(xz)\,dx\right)\omega(z)^{-1}|z|^{1-s}\,d^\times z\end{aligned}$$

כאשר המעבר האחרון מתבצע ע"י שימוש בקשר במידות האר. לבסוף, ראינו כי התבנית $\int_K f(x)\hat{h}(xz)\,dx$ סימטרית בפונקציות f וh ולכן מתקיים כי גם המכפלה $Z(s,h,\omega)Z\left(1-s,\hat{f},\omega^{-1}\right)$ שווה לביטוי זה. ■

מסקנה 16.2 אם $Z(s,f,\omega)$ אינה זהותית אפס אז $Z\left(s,\hat{f},\omega^{-1}\right)$ אינה זהותית אפס: אחרת לכל $h\in\mathcal{S}(K)$ מתקיים $Z\left(1-s,\hat{h},\omega^{-1}\right)$ היא זהותית אפס, כלומר $Z\left(1-s,\varphi,\omega^{-1}\right)$ זהותית אפס לכל $\varphi\in\mathcal{S}(K)$ וראינו שזה לא נכון. (תיארנו את אוסף הפונקציות הנ"ל)

כמו כן, ניתן להגדיר פונקציה מרומורפית $\gamma(s,\omega)$ על K ע"י

$$\gamma(s,\omega) = \frac{Z\left(1-s,\hat{f},\omega^{-1}\right)}{Z(s,f,\omega)}$$

עבור $f\in\mathcal{S}(K)$ כך ש$Z(s,f,\omega)$ אינה זהותית אפס. (בBump ובGoldfeld-Hundley זה מוגדר הפוך)

הערה 16.3 $\gamma(s,\omega)\gamma\left(1-s,\omega^{-1}\right)=\omega(-1)$

הוכחה:

$$\gamma(s,\omega)\gamma\left(1-s,\omega^{-1}\right) = \frac{Z\left(1-s,\hat{f},\omega^{-1}\right)}{Z(s,f,\omega)}\cdot\frac{Z\left(s,\hat{\hat{f}},\omega\right)}{Z\left(1-s,\hat{f},\omega^{-1}\right)}$$

(הביטוי השני במכפלה הוא חישוב γ ע"י שימוש ב$\hat{f}$ במקום בf - כי γ אינה תלוי בבחירת f ואם f אינה זהותית אפס, גם $\hat{f}$ אינה זהותית אפס)

$$\gamma(s,\omega)\gamma\left(1-s,\omega^{-1}\right) = \frac{Z\left(s,\hat{\hat{f}},\omega\right)}{Z(s,f,\omega)}$$

אבל

$$\begin{aligned}
Z\left(s,\hat{\hat{f}},\omega\right) &= \int_{K^\times}\hat{\hat{f}}(x)\,\omega(x)\,|x|^s\,d^\times x\\
&= \int_{K^\times} f(-x)\,\omega(x)\,|x|^s\,d^\times x\\
\underbrace{}_{\substack{y=-x\\ d^\times y=d^\times x}} &= \int_{K^\times} f(y)\,\omega(-y)\,|-y|^s\,d^\times y\\
&= \omega(-1)\,Z(s,f,\omega)
\end{aligned}$$

כנדרש. ■

16.2 תיאור γ

ω **לא מסועף (ואז גם** ω^{-1} **לא מסועף)** נקח $f=\mathrm{Char}_{\mathcal{O}}$, ראינו ש $\hat{f}=f$ ולכן

$$\gamma(s,\omega) = \frac{Z\left(1-s,\mathrm{Char}_{\mathcal{O}},\omega^{-1}\right)}{Z\left(s,\mathrm{Char}_{\mathcal{O}},\omega\right)}=\frac{L\left(1-s,\omega^{-1}\right)}{L(s,\omega)}=\frac{1-\omega(\pi)\,q^{-s}}{1-\omega(\pi)^{-1}\,q^{-(1-s)}}$$

במקרה זה נסמן $\varepsilon=1$.

ω **מסועף (ואז גם** ω^{-1} **מסועף)** במקרה זה $L=1$. ראינו שיש f עם $Z(s,f,\omega)=1$ זהותית ולכן $\gamma\in\mathbb{C}\left[q^s,q^{-s}\right]$. כמו כן יש f כך ש $Z\left(1-s,f,\omega^{-1}\right)=1$ זהותית, ולכן $\gamma^{-1}\in\mathbb{C}\left[q^s,q^{-s}\right]$. לכן יש n שלם ו $a\in\mathbb{C}^\times$ כך ש $\gamma(s,\omega)=aq^{ns}$. במקרה זה מסמנים $\varepsilon(s,\omega)=aq^{ns}$.

סיכום בשני המקרים $\gamma(s,\omega)=\varepsilon(s,\omega)\frac{L(1-s,\omega^{-1})}{L(s,\omega)}$.

הערה 16.4 אפשר להגדיר ε על פי השוויון הנ"ל.

מקרה ארכימדי המשוואה הפונקציונלית נשמרת ע"י אותה הוכחה. נקח $\mathbb{R}$ ונקח $\omega=1$. כאן בדקנו שעבור $f(x)=e^{-\pi x^2}$ מתקיים

$$Z(s,f,1) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)=L_{\mathbb{R}}(s,1)$$

במקרה זה $\hat{f}=f$ ולכן

$$\gamma(s,1) = \frac{Z\left(1-s,\hat{f},1\right)}{Z(s,f,1)}=\frac{L_{\mathbb{R}}(1-s,1)}{L_{\mathbb{R}}(s,1)}=1$$

ולכן $\varepsilon=1$.

17 האדלים של $\mathbb{Q}$: $A_{\mathbb{Q}}$ (Adeles)

17.1 מכפלה טופולוגית מצומצמת (Restricted topological product)

תהי I קבוצת אינדקסים. תהי $\{G_i \mid i\in I\}$ משפחה של חבורות טופולוגיות קומפקטיות מקומית (האוסדורף).

"כמעט לכל i" = "פרט למספר סופי של i-ים".

נניח שכמעט לכל i נתונה תת חבורה $H_i\subseteq G_i$ קומפקטית פתוחה. נגדיר חבורה (מכפלה מצומצמת)

$$\begin{aligned}\prod{}' G_i &= \prod{}'(G_i:H_i)\\ &= \left\{(x_i)_{i\in I}\mid \forall i\,(x_i\in G)\mid x_i\in H_i \text{ for almost every } i\in I\right\}\end{aligned}$$

זו תת־חבורה של חבורת המכפלה $\prod_{i\in I}G_i$.

<u>נגדיר טופולוגיה על $\prod{}'G_i$:</u> נאמר שקבוצת אינדקסים $S\subseteq I$ <u>מותרת</u> אם S סופית וS מכילה כל i עבורו H_i לא מוגדרת.

<u>נסמן:</u>

$$\begin{aligned}G_S &= \left\{(x_i)_{i\in I}\in\prod{}'G_i\mid x_i\in H_i\forall i\in I\setminus S\right\}\\ &\cong \left(\prod_{i\in S}G_i\right)\times\left(\prod_{i\notin S}H_i\right)\end{aligned}$$

נתייחס ל G_S כחבורה טופולוגית קומפקטית מקומית עם טופולוגיית המכפלה. מתקיים

$$\prod{}'G_i = \bigcup_{S\text{ is allowed}} G_S$$

<u>שינוי S:</u> נניח $S\subseteq S_1\subseteq I$ מותרות. אז $G_S\subseteq G_{S_1}$, G_S היא תת־חבורה פתוחה של G_{S_1}. הטופולוגיה על G_S היא הטופולוגיה המושרית מ G_{S_1}.

מסקנה 17.1 קיימת טופולוגיה אחת ויחידה על $\prod{}' G_i$ כך ש

1. $G_S \subseteq \prod{}' G_i$ היא תת־חבורה פתוחה.
2. הטופולוגיה המושרית מ $\prod{}' G_i$ על G_S היא כמו למעלה.

בטופולוגיה הזאת: תהי $\mathcal{O} \subseteq \prod{}' G_i$ פתוחה. אז $\mathcal{O}$ פתוחה ב $\prod{}' G_i$ אם ורק אם $\mathcal{O} \cap G_S$ פתוחה בS לכל S מותרת.

<u>תכונה:</u> $\prod{}' G_i$ חבורה טופולוגית קומפקטית מקומית (כי G_S סביבה פתוחה של 1 לכל S מותרת ו G_S קומפקטית מקומית). בסיס לסביבות של 1 נתון ע"י הקבוצות מהצורה $\prod_{i \in I} U_i$ כך ש

1. U_i סביבה פתוחה של 1_{G_i}
2. $U_i = H_i$ כמעט לכל i.

הערה 17.2 אם $G = \prod'_{i \in I} G_i$ מכפלה מצומצמת לפי $H_i \subseteq G_i$ (כמעט לכל i), אז לכל $i_0 \in I$ ההיטל

$$\begin{aligned} \pi_{i_0} : \prod_{i \in I}{}' G_i &\to G_{i_0} \\ (x_i)_{i \in I} &\mapsto x_{i_0} \end{aligned}$$

רציף.

הוכחה: אכן, לכל $S \subseteq I$ מותרת (כלומר סופית ומכילה כל $i \in I$ עבורו H_i לא מוגדר) ההיטל

$$\pi^S_{i_0} : G_S = \left(\prod_{i \in S} G_i \right) \times \left(\prod_{i \notin S} H_i \right) \to G_{i_0}$$

רציף (כי G_S עם טופולוגיית המכפלה). לכן לכל $U \subseteq G_{i_0}$ פתוחה

$$\pi^{-1}_{i_0}(U) \cap G_S = \left(\pi^S_{i_0} \right)^{-1}(U)$$

פתוחה בG_S, ולפי הגדרת הטופולוגיה על G, נובע ש $\pi^{-1}_{i_0}(U)$ פתוחה בG. ■

17.2 $A_{\mathbb{Q}}$

נסמן $I = \{\infty, 2, 3, 5, \dots\}$ (כלומר I מכיל את ∞ ואת הראשוניים). לכל $\nu = \infty, 2, 3, \dots$ נסמן $G_\nu = \mathbb{Q}_\nu$ (חבורה חיבורית). ו

$$H_\nu = \begin{cases} \mathbb{Z}_p & (\nu = p \text{ is finite}) \\ \text{undefined} & (\nu = \infty) \end{cases}$$

ונגדיר

$$A_{\mathbb{Q}} = \prod_{\nu \in I}{}' \mathbb{Q}_\nu$$

כלומר

$$A_{\mathbb{Q}} \quad = \quad \{(x_\infty, x_2, x_3, \dots) \mid x_p \in \mathbb{Q}_p, x_\infty \in \mathbb{R} \mid x_p \in \mathbb{Z}_p \text{ for almost every } p\}$$

עם טופולוגיה כך שלכל תת־קבוצה סופית $\infty \in S \subseteq I$ הקבוצה

$$(A_{\mathbb{Q}})_S \quad = \quad \left(\prod_{\nu \in S} \mathbb{Q}_\nu\right) \times \left(\prod_{\nu \notin S} \mathbb{Z}_\nu\right)$$

פתוחה, והטופולוגיה המושרית עליה מ $A_{\mathbb{Q}}$ היא טופולוגיית המכפלה.

בסיס לסביבות של $1_{A_{\mathbb{Q}}}$ נתון ע"י קבוצות מהצורה $\left(\prod_{\nu \in S} U_\nu\right) \times \left(\prod_{\nu \notin S} \mathbb{Z}_\nu\right)$ לS מותרת וU_ν סביבה של 1 ב$\mathbb{Q}_\nu$. יחד עם פעולות חיבור וכפל לפי קואורדינטות, $A_{\mathbb{Q}}$ הופך לחוג טופולוגי קומפקטי מקומית.

הערה 17.3 כל ν נקרא מקום (Place).

17.3 השיכון $\mathbb{Q} \subseteq A$

זהו השיכון

$$\begin{array}{rcl} \mathbb{Q} & \hookrightarrow & A \\ r & \mapsto & \left(\underbrace{r}_{\in \mathbb{Q}_\infty}, \underbrace{r}_{\in \mathbb{Q}_2}, \underbrace{r}_{\in \mathbb{Q}_3}, \dots\right) \end{array}$$

תכונות $r \in \mathbb{Q}$ שלם $\iff r \in \mathbb{R} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \dots$. **הוכחה:** אכן, לכל q ראשוני (סופי) נסמן $r = \frac{a}{b} q^n$ עם a, b שלמים הזרים לq, אז $|r|_q = \dfrac{1}{q^n}$ ולכן $r \in \mathbb{Z}_q \iff |r|_q \le 1$ $\iff n \ge 0$. מכאן אם $r \in \mathbb{R} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \dots$ אז לכל q ראשוני מתקיים $r = \frac{a}{b} q^n$ כאשר a, b זרים לq ו$n \ge 0$, ולכן r שלם. ■

מסקנה 17.4 $\mathbb{Q} \cap \left(\left(-\frac{1}{2}, \frac{1}{2}\right) \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \dots\right) = \{0\}$, ומאחר והחלק בסוגריים הוא תת־חבורה פתוחה של A, נובע ש $\mathbb{Q} \subseteq A$ תת־חבורה (ביחס לחיבור) דיסקרטית, ובפרט סגורה.

משפט 17.5 (מקרה פרטי של משפט קירוב בחוגי דדקינד מפרק 10): יהיו $p_1, \dots, p_n$ ראשוניים (סופיים השונים זה מזה) ו $c_i \in \mathbb{Q}_{p_i}$ (ל $i = 1, \dots, n$). אז לכל $\varepsilon > 0$ קיים $r \in \mathbb{Q}$ כך ש

$$(\forall i) \qquad |r - c_i|_{p_i} < \varepsilon$$

וכמו כן יש ייצוג $r = \frac{a}{b}$ כך שהפירוק של b מכיל רק מספרים ראשוניים מתוך $p_1, \dots, p_n$. (כלומר, אם $p \neq p_i$ לכל i, אז $r \in \mathbb{Z}_p$).

הערה 17.6 (ראה גם הוכחה ישירה בGoldfeld-Hundley).

טענה 17.7 תחום יסודי D של $A/\mathbb{Q}$ נתון ע"י

$$\begin{aligned} D &= \{(x_\infty, x_2, \dots) \mid x_\infty \in [0,1), x_p \in \mathbb{Z}_p\} \\ &= [0,1) \times \prod_p \mathbb{Z}_p \end{aligned}$$

הוכחה: יחידות נציג: נניח כי $x, y \in D$ ו $x + \mathbb{Q} = y + \mathbb{Q}$ אז $r = x - y \in \mathbb{Q}$ מתקיים $r \in \mathbb{R} \times \prod_p \mathbb{Z}_p$ ולכן $r \in \mathbb{Z}$, אבל $x, y \in [0,1)$ ו $r = x - y \in \mathbb{Z}$ ולכן $x = y$.
קיום נציג: יהי $x = (x_\infty, x_2, \dots)$. קיימת קבוצה מותרת $S \subseteq \{\infty, 2, 3, \dots\}$ של מקומות כך ש $x_p \in \mathbb{Z}_p$ לכל $p \notin S$ (ואז p סופי). נסמן

$$S = \{\infty, p_1, \dots, p_n\}$$

קיים $r \in \mathbb{Q}$ כך ש $|r - x_{p_i}|_{p_i} < 1$ ל $i = 1, \dots, n$ ו $r \in \mathbb{Z}_p$ (ל$p \notin S$ סופי). אז $x - r \in \mathbb{R} \times \left(\prod_p \mathbb{Z}_p\right)$. לבסוף, יש l סופי כך ש $x_\infty - r - l = (x - r)_\infty - l \in [0,1)$. אז

$$x - (r + l) \in [0,1) \times \left(\prod_p \mathbb{Z}_p\right) = D$$

ו $r + l \in \mathbb{Q}$. ■

מסקנה 17.8 $A/\mathbb{Q}$ קומפקטי.

הוכחה: $\overline{D} = [0,1] \times \prod_p \mathbb{Z}_p$ קומפקטית ואם נסמן ב $\eta : A \to A/\mathbb{Q}$ את ההיטל אז $\eta\left(\overline{D}\right) = A/\mathbb{Q}$. ■

17.4 מידת האר על A

A חבורה טופולוגית (ביחס לחיבור) האוסדורף קומפקטית מקומית, ולכן קיימת לה מידת האר $\mu = \mu_A$. ננרמל את μ כך ש

$$\mu((0,1) \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \dots) = 1$$

(הקבוצה בסוגריים פתוחה עם סגור קומפקטי ולכן מידתה סופית וחיובית)
לכל קבוצת מקומות S מותרת נזכיר סימון

$$A_S = \left(\prod_{\nu \in S} \mathbb{Q}_\nu\right) \times \left(\prod_{\nu = p \notin S} \mathbb{Z}_p\right)$$

והטופולוגיה היא טופולוגיית המכפלה.
כמו כן, $A_S \subseteq A$ תת חבורה פתוחה. לכן צמצום μ על A_S היא מידת האר על A_S. מצד שני, $\prod_{p \notin S} \mathbb{Z}_p$ היא חבורה קומפקטית ויש לה מידת האר μ'' מנורמלת $\mu''\left(\prod_{p \notin S} \mathbb{Z}_p\right) = 1$ ו $\prod_{\nu \in S} \mathbb{Q}_\nu$ מכפלה סופית ויש לה מידת האר הנובעת ממכפלת מידות האר, נסמן אותה ב μ'. נניח ש $\mu'\left((0,1) \times \prod_{\substack{\nu \in S \\ \nu \neq \infty}} \mathbb{Z}_\nu\right) = 1$, אז $\mu = \mu' \times \mu''$.

הערה 17.9 (דוגמה): לכל $t\in\mathbb{R}$ נסמן $A^t=\{(t,x_2,x_3,\dots)\in A\}$, אז $\mu(A^t)=0$ (כי לכל S מתקיים $\mu(A^t\cap A_S)=0$)

17.5 אידלים (Ideles) $A^\times$ (ללא טופולוגיה כרגע)

יהיו $A^\times$ האיברים ההפיכים בA. אם $x=(x_\infty,x_2,\dots)$ אז: $x\in A^\times$ $\Longleftrightarrow$

1. $x_\nu\neq 0$ $(\forall\nu)$
2. $x_p\in\mathbb{Z}_p^\times$ (כלומר $|x_p|_p=1$) כמעט לכל $\nu=p$ סופי. (כי אם x^{-1} קיים, הוא נתון ע"י $\left(x_1^{-1},x_2^{-1},\dots\right)$

מודולוס: לכל $a\in A^\times$ מוגדר $|a|=\prod_\nu|a_\nu|_\nu$. מצד שני, A חוג טופולוגי ולכן עבור $a\in A^\times$

$$\begin{aligned} a\cdot:A &\to A\\ x &\mapsto ax\end{aligned}$$

אוטומורפיזם (טופלוגי) של $\langle A,+\rangle$. לכן מוגדר $\mathrm{mod}_A a\in(0,\infty)$.

טענה 17.10 מתקיים $\mathrm{mod}_A a=|a|$.

הוכחה: נקח $U=(0,1)\times\left(\prod_p\mathbb{Z}_p\right)$, אז $aU=(0,a)\times\left(\prod_p a\mathbb{Z}_p\right)$. כמעט לכל p מתקיים $a\mathbb{Z}_p=\mathbb{Z}_p$ וע"י בחירת S מתאים ופירוק $\mu=\mu'_S\times\mu''_S$ נובע

$$\mathrm{mod}_A a = \mu(a\cdot U)=\prod_\nu|a|_\nu=|a|$$

(לוקחים S כך ש $a\notin\mathbb{Z}_p^\times$ $\Longleftarrow$ $p\in S$) ■

טענה 17.11 (תכונה): אם $r\in\mathbb{Q}^\times$ אז $r\in A^\times$ ו $|r|=1$.

הוכחה: $|\cdot|$ כפלית, ולכן אפשר להניח $r=p$ ראשוני ואז $|p|_p=\frac{1}{p}$, $|p|_{p_i}=1$ $(p_i\neq p)$ ו $|p|_\infty=p$.
(בלי חישוב זה נובע מקומפקטיות $A/\mathbb{Q}$) ■

17.6 פונקציות שוורץ־ברהט על $A=A_\mathbb{Q}$

<u>סימון למכפלת פונקציות:</u> נניח נתונה לכל מקום ν פונקציה $f_\nu:\mathbb{Q}_\nu\to\mathbb{C}$ כך שכמעט לכל ν מתקיים $f_\nu\restriction_{\mathbb{Z}_p}=1$, אז מגדירים

$$\begin{aligned} f=\prod_\nu f_\nu : A &\to \mathbb{C}\\ f(x_\infty,x_2,x_3,\dots) &= \prod_\nu f_\nu(x_\nu)\end{aligned}$$

מינוחים:

- <u>פונקציה מתפרקת:</u> אם $f_\nu\in\mathcal{S}(\mathbb{Q}_\nu)$ לכל ν ואם $f_\nu=\mathrm{Char}_{\mathbb{Z}_\nu}$ כמעט לכל ν, אז נאמר ש $f=\prod_\nu f_\nu$ <u>פונקציה מתפרקת</u>. (Factorizable)
- <u>$\mathcal{S}(A_\mathbb{Q})$ ־ פונקציות שוורץ־ברהט:</u> הצירופים הלינאריים הסופיים (מעל $\mathbb{C}$) של פונקציות מתפרקות מסומן ב$\mathcal{S}(A_\mathbb{Q})$.
- <u>פונקציות אלמנטריות:</u> תהי $f=\prod_\nu f_\nu$ פונקציה מתפרקת. אם לכל ν סופי, מתקיים כי f_ν מהצורה

$$f_\nu=\mathrm{Char}_{a_\nu+\nu^{n_\nu}\mathbb{Z}_\nu}\qquad(a_\nu\in\mathbb{Q}_\nu,n_\nu\in\mathbb{Z})$$

(ואם $f_\nu=\mathrm{Char}_{\mathbb{Z}_\nu}$ כמעט לכל ν), נאמר שf אלמנטרית.

כל פונקציה מתפרקת היא צירוף של פונקציות אלמנטריות ולכן כל $f\in\mathcal{S}(A_\mathbb{Q})$ היא צירוף של פונקציות אלמנטריות.

אינטגרלים של פונקציות מתפרקות על A תהי $f=\prod_\nu f_\nu$ פונקציה מתפרקת. אז

$$\int_A f(x)\,dx=\prod_\nu\int_{\mathbb{Q}_\nu}f_\nu(x_\nu)\,dx_\nu$$

(כאן dx_ν מידה מנורמלת כך שמידת $\mathbb{Z}_p\subseteq\mathbb{Q}_p$ היא 1 ומידת $(0,1)\subseteq\mathbb{Q}_\infty$ היא 1) **הוכחה:** ראשית צד ימין מוגדר, כי $f_p=\mathrm{Char}_{\mathbb{Z}_p}$ כמעט לכל p. יש S מותרת כך שf מתאפסת מחוץ לA_S:

$$A_S=\left(\prod_{\nu\in S}\mathbb{Q}_\nu\right)\times\left(\prod_{\nu=p\notin S}\mathbb{Z}_p\right)$$

לכן לפי הפירוק $\mu=\mu_S'\times\mu_S''$:

$$\begin{aligned}\int_A f(x)\,dx&=\int_{A_S}f(x)\,dx\\&=\int_{\prod_{\nu\in S}\mathbb{Q}_\nu}\prod_{\nu\in S}f_\nu d\mu_S'\times\int_{\prod_{\nu\notin S}\mathbb{Z}_\nu}\underbrace{\prod_{\nu\notin S}f_\nu}_{\mathrm{Char}_{\prod_{\nu\in S}\mathbb{Z}_\nu}}\quad d\mu_S''\end{aligned}$$

לפי הנירמול של μ_S'', הסוגר הימני הוא f. מקבלים לפי פוביני סופי

$$\int_{\prod_{\nu\in S}\mathbb{Q}_\nu}\prod_{\nu\in S}f_\nu d\mu_S'=\prod_{\nu\in S}\int_{\mathbb{Q}_\nu}f_\nu(x_\nu)\,dx_\nu$$

■

18 טרנספורם פוריה על $A = A_{\mathbb{Q}}$

18.1 קרקטר $e : A \to \mathbb{C}^{\times}$

נגדיר $e = \prod_{\nu} e_{\nu}$ על A. כלומר אם $x = (x_{\infty}, x_2, x_3, \dots)$,

$$e(x) = \prod_{\nu} e_{\nu}(x_{\nu})$$

כאשר $e_{\infty}(x_{\infty}) = e^{2\pi i x_{\infty}}$ ו $e_p(x_p) = e^{-2\pi i \{x_p\}}$

הערה 18.1 כמעט לכל p מתקיים $x_p \in \mathbb{Z}_p$ ולכן $e_p(x_p) = 1$ ו $e(x)$ מוגדר, וברור שe קרקטר.

תכונות

1. $e(x+y) = e(x)\, e(y)$
2. $|e(x)| = 1$
3. אם $r \in \mathbb{Q}$ אז $e(r) = 1$

הוכחה: כל מספר רציונלי הוא סכום (או הפרש) של מספרים רציונליים מהצורה $\dfrac{1}{p^k}$ ל $k \geq 1$. (כי אם m, n זרים אז $\frac{1}{m}\mathbb{Z} + \frac{1}{n}\mathbb{Z} = \frac{1}{mn}(n\mathbb{Z} + m\mathbb{Z}) = \frac{1}{mn}\mathbb{Z}$).
נניח כי $r = \frac{1}{p^k}$. אם $p_1 \neq p$ ראשוני (סופי) אז $r \in \mathbb{Z}_{p_1}$ ולכן $e_{p_1}(r) = 1$. מכאן

$$e(r) = e_{\infty}(r)\, e_p(r) = e^{2\pi i \left(r - \{r\}_p\right)}$$

אבל $\{r\}_p = \frac{1}{p^k} = r$ ולכן $r - \{r\}_p = 0$ ו $e(r) = 1$. ■

4. e רציף

הוכחה: נשתמש בסימונים:

נתון כ e_{∞}

$$A_{\mathbb{Q}} \to \mathbb{Q}_{\infty} \xrightarrow{e_{\infty}} \mathbb{C}^{\times}$$

נתון כ $\prod_{p \text{ is finite}} e_p$

$$A_{\mathbb{Q}} \to \prod_{\substack{p \\ p \text{ is finite}}}{}' \mathbb{Q}_p \xrightarrow{\prod_p e_p} \mathbb{C}^{\times}$$

אז $e = e_{\infty} \cdot \prod_p e_p$. אז e_{∞} רציף על $A_{\mathbb{Q}}$ ו $\prod_{p<\infty} e_p$ רציף על $\prod_p \mathbb{Q}_p$ כי הוא שווה ל 1 על התת־חבורה הפתוחה $\mathbb{R} \times \left(\prod_p \mathbb{Z}_p\right)$. ■

18.2 טרנספורם פוריה

הערה 18.2 אם $f=\prod_\nu f_\nu$ פונקציה מתפרקת, אז לכל $y\in A$ הפונקציה

$$\begin{array}{rcl} A & \to & \mathbb{C} \\ x & \mapsto & f(x)\,e(-xy)=\prod_\nu \left(f_\nu(x_\nu)\,e(-x_\nu y_\nu)\right) \end{array}$$

מתפרקת.

הגדרה 18.3 עבור $f\in\mathcal{S}(A_\mathbb{Q})$

$$(y\in A_\mathbb{Q}) \qquad \hat{f}(y)=\int_A f(x)\,e(-xy)\,dx$$

תיאור אפשר להניח $f=\prod_\nu f_\nu$ אלמנטרית.

$$\begin{aligned} \hat{f}(y) &= \int_A \prod_\nu \left(f_\nu(x_\nu)\,e_\nu(-x_\nu y_\nu)\right)dx \\ &= \prod_\nu \int_{\mathbb{Q}_\nu} \left(f_\nu(x_\nu)\,e_\nu(-x_\nu y_\nu)\right)dx_\nu \\ &= \prod_\nu \widehat{f_\nu}(y_\nu) \end{aligned}$$

מסקנה 18.4

1. $\widehat{\prod_\nu f_\nu}=\prod_\nu \widehat{f_\nu}$ (לפונקציות מתפרקות)
2. אם $f\in\mathcal{S}(A_\mathbb{Q})$ אז $\hat{f}\in\mathcal{S}(A_\mathbb{Q})$ ו $\hat{\hat{f}}(x)=f(-x)$ (לכל $x\in A_\mathbb{Q}$)

הזזות ופונקציות אלמנטריות

הערה 18.5 אם K שדה מקומי, $b\in K^\times$ ו $a\in K$ אז

$$(\mathrm{Char}_\mathcal{O})_{a,b} \quad = \quad \mathrm{Char}_{b^{-1}a+b^{-1}\mathcal{O}}$$

(כי $a+bx\in\mathcal{O} \iff x\in -ab^{-1}+b^{-1}\mathcal{O}$)

הגדרה 18.6 (סימון): אם f פונקציה על $A_\mathbb{Q}$ ו $b\in A_\mathbb{Q}^\times$, $a\in A_\mathbb{Q}$ אז נגדיר פונקציה $f_{a,b}$ על $A_\mathbb{Q}$ ע"י

$$(x\in A_\mathbb{Q}) \qquad f_{a,b}(x)=f(a+bx)$$

אם $f=\prod_\nu f_\nu$ מתפרקת, אז

$$\left(\prod_\nu f_\nu\right)_{a,b} \quad = \quad \prod_\nu (f_\nu)_{a_\nu,b_\nu}$$

מתפרקת.

הגדרה 18.7 לכל פונקציית שוורץ (אמיתית)

$$\mathcal{S}(\mathbb{R}) \ni \varphi : \mathbb{R} \rightarrow \mathbb{C}$$

נגדיר $F_\varphi : A \to \mathbb{C}$ ע"י

$$F_\varphi = \varphi \left(\prod_p \mathrm{Char}_{\mathbb{Z}_p} \right)$$

כלומר

$$F_\varphi(x) = \varphi(x_\infty) \cdot \left(\prod_p \mathrm{Char}_{\mathbb{Z}_p}(x_p) \right)$$

טענה 18.8 אם $f = \prod_\nu f_\nu : A \to \mathbb{C}$ פונקציה אלמנטרית, אז קיימים $a \in \mathbb{Q}, b \in \mathbb{Q}^\times$ ו $\varphi \in \mathcal{S}(\mathbb{R})$ כך ש

$$f = (F_\varphi)_{a,b}$$

הוכחה: יש S מותרת, כך שעבור $\nu = p \in S$ סופי

$$f_p = \mathrm{Char}_{a_p + p^{n_p}\mathbb{Z}_p}$$

עבור $p \notin S$:

$$f_p = \mathrm{Char}_{\mathbb{Z}_p}$$

נסמן

$$b = \prod_{p \text{ is finite}} p^{-n_p} \in \mathbb{Q}^\times$$

יהי $a \in \mathbb{Q}$ כך ש

- ל$\nu = p \in S$ סופי: $|a + a_p b| \leq 1$ (כלומר $a + a_p b \in \mathbb{Z}_p$)
- $p \notin S$: a לא מכיל את p במכנה (כלומר $a \in \mathbb{Z}_p$)

אז ל $p \in S$ סופי:

$$\begin{aligned} -b^{-1}a + b^{-1}\mathbb{Z} &= b^{-1}(-a + \mathbb{Z}_p) \\ &= b^{-1}(a_p b + \mathbb{Z}_p) \\ &= a_p + b^{-1}\mathbb{Z}_p \\ &= a_p + p^{n_p}\mathbb{Z}_p \end{aligned}$$

לכן $\left(\mathrm{Char}_{\mathbb{Z}_p}\right)_{a,b} = f_p$.
ל$p \notin S$ מתקיים

$$-b^{-1}a + b^{-1}\mathbb{Z}_p = \mathbb{Z}_p$$

ושוב $\left(\mathrm{Char}_{\mathbb{Z}_p}\right)_{a,b} = f_p$.
לבסוף, כדי לקבל $(F_\varphi)_{a,b} = \prod_\nu f_\nu$ די לקבוע φ כך ש $(\varphi)_{a,b} = f_\infty$. ∎

18.3 נוסחת פואסון

טרנספורם פוריה של הזזה: תהי $f\in\mathcal{S}\left(A\right)$, $a\in A,b\in A^{\times}$.

$$\widehat{f_{a,b}}=\left|b\right|^{-1}e_{\frac{a}{b}}\left(\cdot\right)\cdot\left(\hat{f}\right)_{0,b^{-1}}$$

הוכחה: (בדיקה):

$$\begin{aligned}
\widehat{f_{a,b}}\left(x\right) &= \int_{A}f\left(a+bx\right)e\left(-xy\right)dx\\
&= \int_{A}f\left(a+bx\right)e\left(-bx\frac{y}{b}\right)\frac{d\left(bx\right)}{\left|b\right|}\\
&= \left|b\right|^{-1}\int_{A}f\left(a+x\right)e\left(-x\frac{y}{b}\right)dx\\
&= \left|b\right|^{-1}e\left(\frac{a}{b}y\right)\int_{A}f\left(a+x\right)e\left(-\frac{y}{b}\left(a+x\right)\right)d\left(a+x\right)\\
&= \left|b\right|^{-1}e\left(\frac{a}{b}y\right)\int_{A}f\left(x\right)e\left(-\frac{y}{b}x\right)dx\\
&= \left|b\right|^{-1}e\left(\frac{a}{b}y\right)\hat{f}\left(\frac{y}{b}\right)
\end{aligned}$$

■

משפט 18.9 (נוסחת פואסון): תהי $f\in\mathcal{S}\left(A_{\mathbb{Q}}\right)$ אז

$$\sum_{r\in\mathbb{Q}}f\left(r\right)=\sum_{r\in\mathbb{Q}}\hat{f}\left(r\right)$$

מסקנה 18.10 לכל $b\in A^{\times}$

$$\sum_{r\in\mathbb{Q}}f\left(rb\right)=\frac{1}{\left|b\right|}\sum_{r\in\mathbb{Q}}\hat{f}\left(\frac{r}{b}\right)$$

הוכחה: מנוסחת פואסון

$$\begin{aligned}
\sum_{r\in\mathbb{Q}}f_{0,b}\left(r\right) &= \sum_{r\in\mathbb{Q}}\widehat{f_{0,b}}\left(r\right)\\
&= \sum_{r\in\mathbb{Q}}\left|b\right|^{-1}e_{\frac{0}{b}}\left(r\right)\cdot\left(\hat{f}\right)_{0,b^{-1}}\left(r\right)\\
&= \frac{1}{\left|b\right|}\sum_{r\in\mathbb{Q}}\hat{f}\left(\frac{r}{b}\right)
\end{aligned}$$

■

נעבור להוכחת נוסחת פואסון: **הוכחה:** אפשר להניח שf אלמנטרית. אז קיימים $\varphi\in\mathcal{S}(\mathbb{R})$ ו $a\in\mathbb{Q},b\in\mathbb{Q}^{\times}$ כך ש $f=(F_{\varphi})_{a,b}$. נסמן $F=F_{\varphi}$. אז

$$\begin{aligned}\underbrace{\sum_{r\in\mathbb{Q}}\hat{f}(r)}_{b\in\mathbb{Q}^{\times}} &= \sum_{r\in\mathbb{Q}}\widehat{(F_{a,b})}(r)\\ &= \sum_{r\in\mathbb{Q}}|b|^{-1}e\left(\frac{a}{b}y\right)\hat{F}_{0,b^{-1}}(r)\\ &= \sum_{r\in\mathbb{Q}}\hat{F}\left(\frac{r}{b}\right)\\ &= \sum_{r\in\mathbb{Q}}\hat{F}(r)\end{aligned}$$

(כי $b\in\mathbb{Q}^{\times}$ ולכן $|b|=1$ ו $e_{\frac{a}{b}}(r)=e\left(\frac{a}{b}r\right)=1$ כי $\frac{ar}{b}\in\mathbb{Q}$). מצד שני מתקיים

$$\sum_{r\in\mathbb{Q}}f(r) = \sum_{r\in\mathbb{Q}}F(a+br)=\sum_{r\in\mathbb{Q}}F(r)$$

(כי $a\in\mathbb{Q}$ ו $b\in\mathbb{Q}^{\times}$)

לכן די להוכיח $\sum_{r\in\mathbb{Q}}F(r)=\sum_{r\in\mathbb{Q}}\hat{F}(r)$.

$$\begin{aligned}F &= \varphi\times\mathrm{Char}_{\mathbb{Z}_2}\times\mathrm{Char}_{\mathbb{Z}_3}\times\ldots\\ \hat{F} &= \hat{\varphi}\times\mathrm{Char}_{\mathbb{Z}_2}\times\mathrm{Char}_{\mathbb{Z}_3}\times\ldots\end{aligned}$$

(כי $\widehat{\mathrm{Char}_{\mathbb{Z}_p}}=\mathrm{Char}_{\mathbb{Z}_p}$)

ומכאן נובע שעבור $r\in\mathbb{Q}$

$$\begin{aligned}F(r)\neq0 &\implies \forall p\,(r\in\mathbb{Z}_p)\implies r\in\mathbb{Z}\\ \hat{F}(r)\neq0 &\implies \forall p\,(r\in\mathbb{Z}_p)\implies r\in\mathbb{Z}\end{aligned}$$

ומתקיים

$$\begin{aligned}\sum_{r\in\mathbb{Q}}F(r) &= \sum_{n\in\mathbb{Z}}\varphi(n)\\ \sum_{r\in\mathbb{Q}}\hat{F}(r) &= \sum_{n\in\mathbb{Z}}\hat{\varphi}(n)\end{aligned}$$

ולכן די להוכיח כי $\sum_{n\in\mathbb{Z}}\varphi(n)=\sum_{n\in\mathbb{Z}}\hat{\varphi}(n)$ וזאת נוסחת פואסון הרגילה ל $\varphi\in\mathcal{S}(\mathbb{R})$ שהוכחנו. ■

18.4 טופולוגיה על האידלים

$\mathbb{A}_{\mathbb{Q}}^{\times}$ היא חבורה כפלית, אבל בטופולוגיה המושרה מ$\mathbb{A}_{\mathbb{Q}}$ פונקציית ההופכי אינה רציפה. אכן,

אם נסמן $a_p = \left(\underbrace{1}_{\in\mathbb{R}}, \underbrace{1}_{\in\mathbb{Q}_2}, \dots, 1, \underbrace{p}_{\in\mathbb{Q}_p}, 1, \dots\right)$ אז $a_p \overset{p\to\infty}{\longrightarrow} 1$, אבל $a_p^{-1} \underset{p\to\infty}{\not\longrightarrow} 1$. לכן נגדיר טופולוגיה חדשה על $\mathbb{A}_\mathbb{Q}^\times$.

לכל $p = \nu$ סופי יש תת־חבורה פתוחה וקומפקטית $\mathbb{Z}_p^\times \subseteq \mathbb{Q}_p^\times$.

הגדרה 18.11 נגדיר טופולוגיה על $\mathbb{A}_\mathbb{Q}^\times$ על ידי האיזומורפיזם $\mathbb{A}_\mathbb{Q}^\times \cong \prod_p' \mathbb{Q}_p^\times$ ביחס לתתי החבורות $\mathbb{Z}_p^\times \subseteq \mathbb{Q}_p^\times$, p ראשוני וסופי.

הערה 18.12

1. $\mathbb{A}_\mathbb{Q}^\times \cong \prod_p' \mathbb{Q}_p^\times$ איזומורפיזם של חבורות לפי התכונות שראינו של $\mathbb{A}_\mathbb{Q}^\times$.
2. קיים שיכון של חבורות $j : \mathbb{A}_\mathbb{Q}^\times \hookrightarrow \mathbb{A}_\mathbb{Q} \times \mathbb{A}_\mathbb{Q}$ ע"י $x \mapsto \left(x, x^{-1}\right)$. ניתן להגדיר טופולוגיה על $\mathbb{A}_\mathbb{Q}^\times$ כך שj יהיה שיכון טופולוגי. טופולוגיה זו מזדהה עם הטופולוגיה שהגדרנו.
3. ביחס לטופולוגיה זו, $\mathbb{A}_\mathbb{Q}^\times$ היא חבורה טופולוגית האוסדורף קומפקטית מקומית.

18.5 תחום יסודי עבור $\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times$

נסמן $\mathbb{A}_\mathbb{Q}^\times \supseteq D = (0,\infty) \times \mathbb{Z}_2^\times \times \mathbb{Z}_3^\times \times \dots$ פתוחה.

טענה 18.13 D הוא תחום יסודי עבור $\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times$.

הוכחה: יהי $x = (x_\infty, x_2, \dots) \in \mathbb{A}_\mathbb{Q}^\times$. ע"י כפל ב$-1$ ניתן להניח כי $x_\infty > 0$. תהי $S \subseteq \{\infty, 2, \dots\}$ כך ש $x_p \in \mathbb{Z}_p^\times$ לכל $p \notin S$. לכל $p \in S$ סופי יש $n_p \in \mathbb{Z}$ כך ש $x_p = p^{n_p} \cdot u_p$ ו $u_p \in \mathbb{Z}_p^\times$. ע"י כפל ב $\prod_{\substack{p\in S\\ p \text{ is finite}}} p^{-n_p}$ נקבל ש $x_p \in \mathbb{Z}_p^\times$ לכל p סופי ו $x_\infty > 0$.

אם $q \in \mathbb{Q} \cap D$, אזי $q \in \mathbb{Z}_p^\times$ לכל p ראשוני ולכן $q = \pm 1$ אבל $q > 0$ ולכן $q = 1$.

כיוון ש $D \leq \mathbb{A}_\mathbb{Q}^\times$, D מכילה נציג יחיד מכל מחלקת שקילות. ∎

הערה 18.14 $D \leq \mathbb{A}_\mathbb{Q}^\times$ תת־חבורה פתוחה והטופולוגיה המושרה על D היא טופולוגיית המכפלה $D = (0,\infty) \times \mathbb{Z}_2^\times \times \dots$.

מסקנה 18.15

1. העתקת המנה $\pi : \mathbb{A}_\mathbb{Q}^\times \to \mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times$ משרה איזומורפיזם טופולוגי $D \cong \mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times$.
2. מאחר שD פתוחה, נובע ש $\mathbb{Q}^\times \leq \mathbb{A}_\mathbb{Q}^\times$ דיסקרטית.

3. ראינו שלכל $r \in \mathbb{Q}^{\times}$ מתקיים $|r| = 1$. לכן יש פירוק

$$\begin{array}{ccc}
|\cdot| : \mathbb{A}_{\mathbb{Q}}^{\times} & \longrightarrow & \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \longrightarrow (0,\infty) \\
\cup & \nearrow\cong & \\
D & &
\end{array}$$

$|\cdot| \restriction_D : D \longrightarrow (0,\infty)$.
אם $x = (x_\infty, x_2, \dots) \in D$ אז

$$|x| = |x_\infty|_\infty \cdot \prod_{\substack{p \\ p \text{ is finite}}} |x_p|_p = x_\infty$$

בפרט $|\cdot| \restriction_D$ רציפה, ולכן $|\cdot| : \mathbb{A}_{\mathbb{Q}}^{\times} \to (0,\infty)$ רציפה.

הערה 18.16 נשים לב ש $D \cong \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}$ אינה קומפקטית.

הגדרה 18.17 $\mathbb{A}_{\mathbb{Q}}^{1} = \left\{ x \in \mathbb{A}_{\mathbb{Q}}^{\times} \mid |x| = 1 \right\}$

למה 18.18 $\mathbb{A}_{\mathbb{Q}}^{1} \le \mathbb{A}_{\mathbb{Q}}$ סגורה ו $\mathbb{Q}^{\times} \le \mathbb{A}_{\mathbb{Q}}^{1}$ דיסקרטית. כמו כן, יש איזומורפיזם

$$\mathbb{A}_{\mathbb{Q}}^{1}/\mathbb{Q}^{\times} \cong \left(\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}\right)^{1} = \left\{ \gamma \in \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \mid |\gamma| = 1 \right\}$$

מסקנה 18.19 $\mathbb{A}_{\mathbb{Q}}^{1}/\mathbb{Q}^{\times} \cong \prod_{\substack{p \\ p \text{ is finite}}} \mathbb{Z}_p^{\times}$ ובפרט $\mathbb{A}_{\mathbb{Q}}^{1}/\mathbb{Q}^{\times}$ חבורה קומפקטית.

18.6 מידת האר על $\mathbb{A}_{\mathbb{Q}}^{\times}$

על $\mathbb{Z}_2^{\times} \times \mathbb{Z}_3^{\times} \times \dots$ יש מידת האר יחידה μ_t כך שמתקיים $\mu_t\left(\mathbb{Z}_2^{\times} \times \mathbb{Z}_3^{\times} \times \dots\right) = 1$. תהי μ_L מידת האר על $(0,\infty)$ כך שמתקיים $\mu_L(1,2) = \ln 2$. אז $\mu = \mu_L \times \mu_t$ מידת האר על D. כיוון שD תת־חבורה פתוחה של $\mathbb{A}_{\mathbb{Q}}^{\times}$ שמרחיבה את μ מD. נסמן אותה בμ.

מסקנה 18.20

1. עבור $f : \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \longrightarrow [0,\infty]$ מדידה מתקיים

$$\begin{aligned}
\int_{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}} f(x)\, d\mu(x) &= \int_D f(x)\, d\mu(x) \\
&= \int_0^\infty \left[\int_{\prod_{p<\infty} \mathbb{Z}_p^{\times}} f(x_\infty, x_t)\, d\mu_t(x_t) \right] \frac{dx_\infty}{x_\infty}
\end{aligned}$$

כאשר $x = (x_\infty, x_2, \dots)$ ו $x_t = (x_2, \dots)$. בפרט $\mu\left(\{t\} \times \left(\prod_{p<\infty} \mathbb{Z}_p^{\times}\right)\right) = 0$.

2. <u>למה על פירוק אינטגרלים:</u> תהי $f_\nu : \mathbb{Q}_\nu^\times \to \mathbb{C}$ פונקציה אינטגרבילית. נניח שכמעט לכל p סופי $f\restriction_{\mathbb{Z}_p^\times}=1$ ושמתקיים $\prod_p \int_{\mathbb{Q}_p^\times} |f_p|\, d\mu_p^\times < \infty$.
אז $f=\prod f_\nu : \mathbb{A}_\mathbb{Q}^\times \to \mathbb{C}$ אינטגרבילית על $\mathbb{A}_\mathbb{Q}^\times$ ומתקיים

$$\int_{\mathbb{A}_\mathbb{Q}^\times} f(x)\, d\mu(x) = \prod_\nu \int_{\mathbb{Q}_\nu^\times} f_\nu(x_\nu)\, d\mu_\nu^\times(x)$$

הוכחה: ברור שf מוגדרת היטב. תהי $S_1 \subseteq S_2 \subseteq \ldots$ סדרת קבוצות מותרות כך ש $f_p\restriction_{\mathbb{Z}_p^\times}=1$ לכל $p\notin S_1$ וכך ש $\bigcup S_n = \{\infty, 2, \ldots\}$.
לכל $p\notin S_n$ מתקיים $|f_p| \geq \mathrm{Char}_{\mathbb{Z}_p^\times}$ ומכאן נובע שמתקיים

$$\left(\prod_{\nu\in S_n} |f_\nu|\right)\times\left(\prod_{p\notin S_n}\mathrm{Char}_{\mathbb{Z}_p^\times}\right) \nearrow |f| = \prod_\nu |f_\nu|$$

לכן ממשפט ההתכנסות המונוטונית מתקיים

$$\begin{aligned}
\int_{\mathbb{A}_\mathbb{Q}^\times} |f(x)|\, d\mu(x) &= \lim_{n\to\infty}\int_{\mathbb{A}_\mathbb{Q}^\times}\prod_{\nu\in S_n}|f_\nu|\times\prod_{p\notin S_n}\mathrm{Char}_{\mathbb{Z}_p^\times}\, d\mu \\
&= \lim_{n\to\infty}\int_{\prod_{\nu\in S_n}\mathbb{Q}_\nu^\times\times\prod_{p\notin S_n}\mathbb{Z}_p^\times}\prod_{\nu\in S_n}|f_\nu|\, d\mu \\
&= \lim_{n\to\infty}\int_{\prod_{\nu\in S_n}\mathbb{Q}_\nu^\times}\prod_{\nu\in S_n}|f_\nu|\, d\prod_{\nu\in S_n}\mu_\nu^\times \\
&= \lim_{n\to\infty}\prod_{\nu\in S_n}\int_{\mathbb{Q}_\nu^\times}|f_\nu|\, d\mu_\nu^\times \\
&= \prod_\nu\int_{\mathbb{Q}_\nu^\times}|f_\nu|\, d\mu_\nu^\times < \infty
\end{aligned}$$

כאשר האי־שוויון האחרון נובע מהנתון. בפרט $f(x)$ אינטגרבילית. מתקיים

$$A_n = \prod_{\nu\in S_n}\mathbb{Q}_\nu^\times\times\prod_{\nu\notin S_n}\mathbb{Z}_\nu^\times \nearrow \mathbb{A}_\mathbb{Q}^\times$$

ולכן

$$\begin{aligned}
\int_{\mathbb{A}_\mathbb{Q}^\times} f(x)\, d\mu(x) &= \lim_{n\to\infty}\int_{A_n}\prod_\nu f_\nu d\mu \\
&= \lim_{n\to\infty}\int_{\prod_{\nu\in S_n}\mathbb{Q}_\nu^\times}\prod_{\nu\in S_n} f_\nu d\left(\prod_{\nu\in S_n}\mu_\nu^\times\right) \\
&= \lim_{n\to\infty}\prod_{\nu\in S_n}\int_{\mathbb{Q}_\nu^\times} f_\nu d\mu_\nu^\times
\end{aligned}$$

כנדרש. ■

18.7 קרקטרים על $\mathbb{A}_{\mathbb{Q}}^{\times}$

יהי $\eta:\mathbb{A}_{\mathbb{Q}}^{\times}\to\mathbb{C}^{\times}$ קרקטר רציף. לכל ν יש שיכון טופולוגי

$$\begin{array}{rcl} j_{\nu}:\mathbb{Q}_{\nu}^{\times} & \to & \mathbb{A}_{\mathbb{Q}}^{\times}\\ x_{\nu} & \mapsto & \left(1,\dots,x_{\nu},1,\dots\right)\end{array}$$

ולכן לכל ν נקבל קרקטר רציף

$$\eta_{\nu} = \eta\circ j_{\nu}$$

נשים לב שη_{ν} לא מסועף כמעט לכל ν.

מסקנה 18.21 לכל $x=\left(x_{\infty},x_{2},\dots\right)$ מתקיים $\eta\left(x\right)=\prod_{\nu}\eta_{\nu}\left(x_{\nu}\right)$. נסמן $\eta=\prod\eta_{\nu}$.

הערה 18.22 בכיוון ההפוך, אם לכל ν יש $\eta_{\nu}:\mathbb{Q}_{\nu}^{\times}\to\mathbb{C}^{\times}$ וη_{ν} לא מסועף כמעט לכל ν, אזי $\eta=\prod\eta_{\nu}$ קרקטר רציף של $\mathbb{A}_{\mathbb{Q}}^{\times}$.

למה 18.23 יהי $\omega:\mathbb{A}_{\mathbb{Q}}^{\times}\to\mathbb{C}^{\times}$ קרקטר אוניטרי רציף. תהי $f:\mathbb{A}_{\mathbb{Q}}\to\mathbb{C}$ פונקציית שוורץ. אז לכל $s\in\mathbb{C}$ האינטגרל

$$\int_{\substack{x\in\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}\\ |x|\geq1}}\left(\sum_{\alpha\in\mathbb{Q}^{\times}}f\left(\alpha x\right)\right)\omega\left(x\right)\left|x\right|^{s}d\mu^{\times}\left(x\right)$$

מתכנס בהחלט ומתאר פונקציה שלמה של s.

19 החישוב היסודי

19.1 קרקטר הקה ואינטגרל זיטא גלובלי

הגדרה 19.1 קרקטר הקה הוא קרקטר רציף $\omega:\mathbb{A}_{\mathbb{Q}}^{\times}\to\mathbb{C}^{\times}$ כך ש $\omega\restriction_{\mathbb{Q}^{\times}}=1$.

הגדרה 19.2 יהי ω קרקטר הקה, $f\in\mathcal{S}\left(\mathbb{A}_{\mathbb{Q}}\right)$. פונקציית זיטא גלובלית היא

$$Z\left(s,f,\omega\right) = \int_{\mathbb{A}_{\mathbb{Q}}^{\times}}f\left(x\right)\omega\left(x\right)\left|x\right|_{\mathbb{A}_{\mathbb{Q}}}^{s}d\mu\left(x\right)$$

הערה 19.3 יש פירוק $\omega=\prod_{\nu}\omega_{\nu}$ וכמעט לכל ν, ω_{ν} לא מסועף. כמו כן, ω נקבע באופן יחיד על ידי $\omega\restriction_{D}:D\to\mathbb{C}^{\times}$, $D=\left(0,\infty\right)\times\mathbb{Z}_{2}^{\times}\times\dots$. לגבי $\left(0,\infty\right)$ קיים $s_{0}\in\mathbb{C}$ יחיד כך ש $\omega_{\infty}\left(t\right)=t^{s_{0}}$, $t\in\mathbb{R}_{\geq0}$. נשים לב ש

$$\omega\left(t,1,\dots\right) = \omega_{\infty}\left(t\right)=t^{s_{0}}=\left|\left(t,1,\dots\right)\right|^{s_{0}}$$

לכן על ידי הזזה בs, ניתן להניח כי $\omega_{\infty}\equiv1$. (מעטה נניח זאת). בפרט ω אוניטרי.

הערה 19.4 במצב זה יש שקילויות:

1. $\omega\equiv1$
2. ω_p לא מסועף לכל p סופי
3. ω_ν לא מסועף לכל ν

הוכחה: $1\Longleftarrow3\Longleftarrow2$: ברור.
$2\Longleftarrow1$: די להראות כי $\omega_p(p)=1$ ו $\omega_\infty(-1)=1$. אבל

$$\omega(p) = \omega_\infty(p)\cdot\left(\prod_{p_1\neq p}\omega_{p_1}(p)\right)\cdot\omega_p(p)$$

כעת $\omega_\infty(p)=1$ כי $p>0$ ו $\omega_{p_1}(p)=1$ כי ω_{p_1} לא מסועף. באופן דומה עבור $\omega_\infty(-1)$.
■

חישוב עזר נסמן

$$I(M) = \int_{\substack{x\in\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times\\|x|\leq1}}\omega(x)\cdot|x|^M\,d\mu(x)$$

כאשר $\mathrm{Re}(M)>0$. מתקיים

$$\left\{x\in\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times\mid|x|\leq1\right\} = (0,1]\times\mathbb{Z}_2^\times\times\ldots$$

התכנסות בהחלט:

$$\begin{aligned}\int_{\substack{x\in\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times\\|x|\leq1}}|x|^{\mathrm{Re}(M)}\,d\mu(x) &= \int_{(0,1]\times\mathbb{Z}_2^\times\times\ldots}|x_\infty|^{\mathrm{Re}(M)}\,d\left(\mu_\infty\times\mu_{\mathbb{Z}_2^\times}\times\ldots\right)\\ &= \int_0^1x^{\mathrm{Re}(M)}\frac{dx}{x}\\ &= \frac{1}{\mathrm{Re}(M)}<\infty\end{aligned}$$

לכן $I(M)$ מתכנס בהחלט עבור $\mathrm{Re}(M)>0$ ואם $\omega=1$ אז $I(M)=\frac{1}{M}$. אם $\omega\neq1$ האינטגרל הוא אפס כי יש p סופי כך שω_p מסועף, כלומר $\omega\restriction_{\mathbb{Z}_p^\times}\not\equiv1$ ואז $\int_{\mathbb{Z}_p^\times}\omega_p(x)\,d\mu_p(x)=0$ ומכאן $I(M)=0$.

19.2 פונקציות L

הגדרה 19.5 בסימונים אלה פונקציית-L (Completed L-function) היא

$$L(s,\omega) = \prod_\nu L_\nu(s,\omega_\nu)$$

נסמן ב $\{2,3,\dots\} \subseteq S$ את אוסף המקומות כך שω_p מסועף. אם ω_p מסועף אז $L_p(s,\omega_p)=1$ ולכן

$$L(s,\omega) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\prod_{p\notin S}\left(1-\omega_p(p)\,p^{-s}\right)^{-1}$$

(נניח כי $\omega_\infty(-1)=1$)
המכפלה מתכנסת עבור $\mathrm{Re}s>1$ כי ω_p אוניטרי.

מקרה פרטי אם $\omega\equiv 1$ אז $S=\emptyset$ ואז $L(s,1)=\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$.

19.3 פירוק אינטגרל זיטא

נבחר $\mathcal{S}(\mathbb{A}_{\mathbb{Q}}) \ni f=\prod_\nu f_\nu$ מתפרקת כך ש:

1. $f_\infty(t)=e^{-\pi t^2}$, $t\in\mathbb{R}$.
2. אם ω_p לא מסועף ניקח $f_p=\mathrm{Char}_{\mathbb{Z}_p}$.
3. אם ω_p מסועף ניקח f_p כך ש $Z_p(s,f_p,\omega_p)$ אינו אפס. (ניתן להניח $Z_p(s,f_p,\omega_p)=1$)

בתנאים אלו ניתן להשתמש בלמה על פירוק אינטגרלים עבור $Z(s,\omega)=\int_{\mathbb{A}_{\mathbb{Q}}^\times} f(x)\,\omega(x)\,|x|^s\,d\mu(x)$ כי $f(x)\,\omega(x)\,|x|^s$ מתפרקת. נקבל עבור $\mathrm{Re}s>1$ כי

$$\begin{aligned}
Z(s,f,\omega) &= \prod_\nu Z_\nu(s,f_\nu,\omega)\\
&= \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\cdot\prod_{p\in S}Z_p(s,f_p,\omega_p)\cdot\prod_{p\notin S}\left(1-\omega_p(p)\,p^{-s}\right)^{-1}\\
&= \prod_{p\in S}Z_p(s,f_p,\omega_p)\cdot L(s,\omega)
\end{aligned}$$

הערה 19.6 אם $\omega\equiv 1$ אז $Z(s,f,1)=L(s,1)$.
אם ניקח f כך ש $Z_p(s,f_p,\omega_p)=1$ נקבל כי $Z(s,f,\omega)=L(s,\omega)$.

19.4 החישוב היסודי

בסימונים הללו, עבור $\mathrm{Re}(s)>1$ ומאחר ש $\mathbb{Q}^\times\subseteq\mathbb{A}_{\mathbb{Q}}^\times$ דיסקרטית

$$\begin{aligned}
Z(s,f,\omega) &= \int_{\mathbb{A}_{\mathbb{Q}}^\times} f(x)\,\omega(x)\,|x|^s\,d\mu(x)\\
&= \int_{\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times}\sum_{\alpha\in\mathbb{Q}^\times} f(\alpha x)\,\omega(\alpha x)\,|\alpha x|^s\,d\mu(x)\\
&= \int_{\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times}\left(\sum_{\alpha\in\mathbb{Q}^\times} f(\alpha x)\right)\omega(x)\,|x|^s\,d\mu(x)
\end{aligned}$$

השוויון נכון כי $|\alpha| = 1$ לכל $\alpha \in \mathbb{Q}^{\times}$ (ראינו). $\omega(\alpha) = 1$ לכל $\alpha \in \mathbb{Q}$ כי ω הקה.
נשתמש בנוסחת פואסון ונקבל שלכל $x \in \mathbb{A}_{\mathbb{Q}}^{\times}$ מתקיים

$$\sum_{\alpha \in \mathbb{Q}} f(rx) = \frac{1}{|x|} \sum_{r \in \mathbb{Q}} \hat{f}\left(\frac{r}{x}\right)$$

ולכן

$$\sum_{\alpha \in \mathbb{Q}^{\times}} f(\alpha x) = -f(0) + \frac{1}{|x|}\hat{f}(0) + \frac{1}{|x|} \sum_{\alpha \in \mathbb{Q}^{\times}} \hat{f}\left(\frac{\alpha}{x}\right)$$

נקבל כי

$$Z(s,f,\omega) = \int_{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}} \left(-f(0) + \frac{\hat{f}(0)}{|x|} + \sum_{\alpha \in \mathbb{Q}^{\times}} \hat{f}\left(\frac{\alpha}{x}\right)\frac{1}{|x|}\right) \omega(x)|x|^{s} d\mu(x)$$

מתקיים $d\mu\left(\frac{1}{x}\right) = d\mu(x)$ ולכן נקבל

$$\begin{aligned}
Z(s,f,\omega) &= \int_{\substack{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \\ |x|\geq 1}} \left(\sum_{\alpha \in \mathbb{Q}^{\times}} f(\alpha x)\right) \omega(x)|x|^{s} d\mu(x) + \\
& \int_{\substack{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \\ |x|\leq 1}} \left(-f(0) + \frac{\hat{f}(0)}{|x|} + \sum_{\alpha \in \mathbb{Q}^{\times}} \frac{1}{|x|}\hat{f}\left(\frac{\alpha}{x}\right)\right) \omega(x)|x|^{s} d\mu(x) \\
&= \int_{\substack{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \\ |x|\geq 1}} \left(\sum_{\alpha \in \mathbb{Q}^{\times}} f(\alpha x)\right) \omega(x)|x|^{s} d\mu(x) + \\
& \int_{\substack{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \\ |x|\geq 1}} \left(\sum_{\alpha \in \mathbb{Q}^{\times}} \hat{f}(\alpha x)|x|\right) \overline{\omega}(x)|x|^{-s} d\mu(x) + \\
& \int_{\substack{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \\ |x|\leq 1}} \left(-f(0) + \frac{\hat{f}(0)}{|x|}\right) \omega(x)|x|^{s} d\mu(x) \\
&= \int_{\substack{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \\ |x|\geq 1}} \left(\sum_{\alpha \in \mathbb{Q}^{\times}} f(\alpha x)\omega(x)|x|^{s} + \sum_{\alpha \in \mathbb{Q}^{\times}} \hat{f}(\alpha x)\overline{\omega}(x)|x|^{1-s} d\mu(x)\right) + \\
& \int_{\substack{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times} \\ |x|\leq 1}} \left(-f(0)|x|^{s} + \hat{f}(0)|x|^{s-1}\right) \omega(x) d\mu(x)
\end{aligned}$$

מהלמה, האינטגרל הראשון מתאר פונקציה שלמה. האינטגרל השני מתכנס עבור $\mathrm{Re}s > 1$

ומתקיים ש

$$\int_{\substack{\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}\\|x|\le1}}\left(-f(0)|x|^{s}+\hat{f}(0)|x|^{s-1}\right)\omega(x)\,d\mu(x) = \begin{cases}0 & \omega\not\equiv1\\ -\frac{f(0)}{s}+\frac{\hat{f}(0)}{s-1} & \omega\equiv1\end{cases}$$
$$= \begin{cases}0 & \omega\not\equiv1\\ -\left(\frac{1}{s}+\frac{1}{1-s}\right) & \omega\equiv1\end{cases}$$

(לבדוק שאכן $\hat{f}(0)=1$)

משפט 19.7 עבור f לעיל, ל$Z(s,f,\omega)$ יש המשכה אנליטית לפונקציה שלמה עבור $\omega\not\equiv1$ ולפונקציה מרומורפית עם קטבים פשוט ב$s=0,1$ עבור $\omega\equiv1$. בשני המקרים מתקיימת המשוואה הפונקציונלית

$$Z(s,f,\omega) = Z\left(1-s,\hat{f},\overline{\omega}\right)$$

יישום לזיטא ניקח $\omega\equiv1$. קיבלנו כי $Z(s,f,\omega)=\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ ופונקציה זו אינווריאנטית לשיקוף $s\mapsto1-s$.

יישום ל$L(s,\omega)$, $\omega\not\equiv1$ ראשית, ניקח f שמקיימת $Z_p(s,f_p,\omega_p)=1$, ואז $Z(s,f,\omega)=L(s,\omega)$ ולכן $L(s,\omega)$ היא פונקציה שלמה.

המשוואה הפונקציונאלית של פונקציות־L של הקה יהי $p\in S$, כלומר ω_p מסועף, אזי

$$\frac{L_p\left(1-s,\hat{f},\omega_p\right)}{L_p(s,f,\omega_p)} = \gamma_p(s,\omega_p)=\varepsilon(s,\omega_p)$$

ומתקיים $\varepsilon_p(s,\omega_p)=a_p\cdot b_p^{s}$ עם $a_p\in\mathbb{C}^{\times}$ ו $b_p>0$.
נסמן $\varepsilon(s,\omega)=\prod_{p\in S}\varepsilon_p(s,\omega_p)$ (מהצורה $a\cdot b^{s}$), אז מהמשוואה הפונקציונאלית של אינטגרל זיטא נקבל כי

$$\left(\prod_{p\in S}Z_p(s,f_p,\omega_p)\right)\cdot L(s,\omega) = \left(\prod_{p\in S}Z_p\left(1-s,\hat{f}_p,\overline{\omega}_p\right)\right)\cdot L(1-s,\overline{\omega})$$

לכן נקבל כי $L(s,\omega)=\varepsilon(s,\omega)\cdot L(1-s,\overline{\omega})$.

טורי דיריכלה

הגדרה 19.8 פונקציה $\chi:\mathbb{Z}\to\mathbb{C}$ נקראת קרקטר דיריכלה אם קיימים $N\ge1$ טבעי וקרקטר $\chi_0:(\mathbb{Z}/N\mathbb{Z})^{\times}\to\mathbb{C}^{\times}$ כך ש

$$\chi(n) = \begin{cases}\chi_0(n+N\mathbb{Z}) & \gcd(n,N)=1\\ 0 & \text{else}\end{cases}$$

אם ניתן למצוא N וχ_0 כך שאין $N' \mid N$, $N \neq N'$ וקרקטר $\chi_0' : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, כך $\chi_0 = \chi_0' \circ \pi$ אז נאמר שχ קרקטר דיריכלה פרימיטיבי.

הערה 19.9 נניח שקיימים N', χ_0' כנ"ל ונבנה χ' לפי N', χ_0'. אזי ההבדל בין $\chi(n)$ ל$\chi'(n)$ הוא:

1. אם $(n,N)=1$ אז $\chi(n)=\chi'(n)$
2. אם $(n,N')=1$ ו$(n,N)\neq 1$ אז $\chi(n)=0$ ו $\chi'(n)\neq 0$
3. אם $(n,N')\neq 1$ אז $\chi(n)=\chi'(n)=0$

בפרט אם לN, N' אותם גורמים ראשוניים, אז $\chi=\chi'$.

תכונות

1. $\chi(1)=1$
2. $|\chi(n)|=1,0$
3. $\chi(nm)=\chi(n)\chi(m)$
4. אם $N=1$ נגדיר $\chi(n)=1$ לכל n.

בניית קרקטר דיריכלה פרימיטיבי יהי $n=p_1^{n_1}\cdot\dots\cdot p_l^{n_l}$ ראשוניים שונים זה מזה, $n_i\geq 1$. יהיו $\chi_{i,0} : (\mathbb{Z}/p^{n_i}\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ קרקטרים לא טריוואלים. מתוך $\mathbb{Z}/N\mathbb{Z}\cong\prod_i\left(\mathbb{Z}/p^i\mathbb{Z}\right)$ נקבל $(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \prod_i\left(\mathbb{Z}/p^i\mathbb{Z}\right)^\times$ ואז נקבל $\chi_0=\prod_i\chi_{i,0}$.
יהי χ קרקטר דיריכלה שנבנה לפי χ_0. אז χ קרקטר דיריכלה פרימיטיבי.

הגדרה 19.10 יהי χ קרקטר פרימיטיבי. נבנה בעזרת χ,N פונקציית L המתאימה לχ על ידי

$$L(s,\chi) = \prod_{\substack{p\nmid N\\ p\text{ is prime}}}\left(1-\chi(p)p^{-s}\right)^{-1}$$

הערה 19.11 עבור $\mathrm{Re}s>1$, $L(s,\chi)$ פונקציה אנליטית ומתקיים

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

מצד שני, לכל קרקטר הקה $\omega:\mathbb{A}_{\mathbb{Q}}^\times\to\mathbb{C}^\times$ כך שω אוניטרי נתייחס ל

$$\begin{aligned}
L'(s,\omega) &= \prod_{p\text{ is finite}} L(s,\omega_p)\\
&= \prod_{\substack{p\text{ is finite}\\ p\notin S}}\left(1-\omega_p(p)p^{-s}\right)
\end{aligned}$$

טענה 19.12 האוסף $L'(s,\omega)$ זהה לאוסף $L(s,\omega)$ של קרקטרי דיריכלה פרימיטיביים.

למה 19.13 יש איזומורפיזם $\left(\mathbb{Z}/p^{n}\mathbb{Z}\right)^{\times} \cong \mathbb{Z}_p^{\times}/\left(1+p^{n}\mathbb{Z}_p^{\times}\right)$

בניית קרקטר הקה נחזור ל $D \cong \mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}$, $D \leq \mathbb{A}_{\mathbb{Q}}^{\times}$ תת־חבורה פתוחה ולכן יש איזומורפיזם טופולוגי $\mathbb{Q}^{\times} \times D \cong \mathbb{A}_{\mathbb{Q}}^{\times}$.
לכן, יש התאמה בין קרקטרי הקה לקרקטרים אוניטריים על D, ולכן התאמה לקרקטרים רציפים אוניטריים $\omega : \prod_{p\neq\infty}\mathbb{Z}_p^{\times} \to \mathbb{C}$.

בנייה נבנה קרקטר הקה $\omega \not\equiv 1$.
תהי $S \subseteq \{2,3,\dots\}$ סופית. לכל $p \in S$ יהי $\omega_p : \mathbb{Z}_p^{\times} \longrightarrow \mathbb{C}$ קרקטר רציף לא טריוואלי.
כך נקבל

$$\prod_{p\in S}\omega_p : \prod_{p\in S}\mathbb{Z}_p^{\times} \longrightarrow \mathbb{C}^{\times}$$

נרחיב לקרקטר רציף

$$\omega : \prod_{p\neq\infty}\mathbb{Z}_p^{\times} \longrightarrow \mathbb{C}^{\times}$$

כך ש$\omega_p \equiv 1$ לכל $p \notin S$. נרחיב את ω לקרקטר הקה אוניטרי $\omega : \mathbb{A}_{\mathbb{Q}}^{\times} \to \mathbb{C}^{\times}$, כך מקבלים את כל קרקטרי הקה השונים מ1.
נבחן את ω_p. יהי $p^{n_p}\mathbb{Z}_p$ המוביל של ω_p. אזי $n_p \geq 1$ כי $\omega_p \not\equiv 1$, וω_p משרה קרקטר על $\left(\mathbb{Z}/p^{n_p}\mathbb{Z}\right)^{\times} \cong \mathbb{Z}_p^{\times}/\left(1+p^{n_p}\mathbb{Z}_p^{\times}\right)$.
לכן יש דיאגרמה

$$\begin{array}{ccccc}
\mathbb{Z}_p^{\times} & \longrightarrow & \mathbb{Z}_p^{\times}/\left(1+p^{n_p}\mathbb{Z}_p^{\times}\right) & \longrightarrow & \mathbb{C}^{\times} \\
?\uparrow & & \cong\uparrow & \nearrow \xi_p & \\
\mathbb{Z} & & \left(\mathbb{Z}/p^{n_p}\mathbb{Z}\right)^{\times} & &
\end{array}$$

נסמן $N = \prod p^{n_p}$ ונגדיר $\xi : \left(\mathbb{Z}/N\mathbb{Z}\right)^{\times} \longrightarrow \mathbb{C}^{\times}$ על ידי $\xi = \prod_p \xi_p$. אז ξ קרקטר וω,ξ קובעים זה את זה.
לכל $p \notin S$ מתקיים

$$\begin{aligned}
1 &= \omega(p) \\
&= \omega_\infty(p)\cdot\prod_{p_1\in S}\omega_{p_1}(p)\cdot\prod_{p_1\notin S}\omega_{p_1}(p) \\
&= \prod_{p_1\in S}\xi_{p_1}(p)\cdot\omega_p(p) \\
&= \xi(p)\cdot\omega_p(p)
\end{aligned}$$

מכאן נובע $\omega_p(p) = \xi^{-1}(p)$, לכל $p \in S$, כנדרש.