תורת המספרים האלגברית

תוכן העניינים

1 שדות מספרים 2
1.1 הרחבות שלמות 2
1.2 שדות מספרים 3
1.3 הדיסקרימיננטה 6

2 תחומי דדקינד 8
2.1 פירוק אידאלים בתחום דדקינד 9
2.2 אידאלים שבריים וחבורת המחלקות 10
2.3 הנורמה של אידאל 11
2.4 שריגים 13
2.5 חסם מינקובסקי ומספר המחלקות 15
2.6 משפט היחידות של דיריכלה 18

3 אידאלים ראשוניים בתחומי דדקינד 21
3.1 הסתעפות של ראשוניים בשדות מספרים 21
3.2 פירוק של אידאלים ראשוניים בהרחבות של תחומי דדקינד 23
3.3 הסתעפות בהרחבות גלואה 27
3.4 השדות הציקלוטומיים 29

4 הערכות (וליואציות) 32
4.1 שדות עם הערכה 32
4.2 ההשלמה של שדה ביחס להערכה 35
4.3 חוג השלמים, שדה השאריות והלמה של הנזל 37
4.4 הערכות והרחבות שדות 42
4.5 הערכות אקספוננציאליות 45
4.6 שדות הנזליים 47
4.7 יישומים ללמידת $\mathbb{Q}_p$ 49
4.8 הסתעפות בהרחבות של שדה הנזלי 50
4.9 משפט הרברנד 55

5 הקדמה לתורת שדות המחלקות 57
5.1 מבוא לקוהומולוגיה של חבורות 58
5.2 דוגמת שימוש: חבורת בראוור של הרחבות של $\mathbb{Q}_p$ 60
5.3 דואליות פואנקרה 62
5.4 תוכנית לנגלנדס 63

בקורס שלנו, כל החוגים קומוטטיביים ומכילים איבר יחידה.

1 שדות מספרים

1.1 הרחבות שלמות

יהי $x \in \mathbb{Q}$. אנחנו יודעים כי $x \in \mathbb{Z}$ אם ורק אם הוא שורש של פולינום מתוקן מעל $\mathbb{Z}$. זה מוביל להגדרה הבאה:

הגדרה 1.1. יהי A תחום שלמות, ותהי B אלגברה מעל A.

א. איבר $b \in B$ נקרא **אלגברי** (**algebraic**) מעל A, אם קיימים $a_0, a_1, \dots, a_n \in A$ (לא כולם 0) שעבורם $a_n b^n + \dots + a_1 b + a_0 = 0$.

ב. איבר $b \in B$ נקרא **שלם** (**integral**) מעל A, אם ניתן לקחת $a_n = 1$.

הגדרה 1.2. יהי A תחום שלמות, ותהי L אלגברה מעל A. ה**סגור השלם** (**integral closure**) של A ב-L הינו

$$\{x \in L : x \text{ שלם מעל } A\} \subseteq L .$$

טענה 1.3. יהי A תחום שלמות, תהי B אלגברה מעל A, ויהי $b \in B$. התנאים הבאים שקולים:

א. b שלם מעל A.

ב. תת-האלגברה $A[b] \subseteq B$ נוצרת סופית כ-A-מודול.

ג. קיימת תת-אלגברה $S \subseteq B$ כך ש-$b \in S$ ו-S נוצרת סופית כ-A-מודול.

ד. קיים תת-A-מודול נוצר סופית M של B כך ש-$bM \subseteq M$ ו-M נאמן מעל $A[b]$.

הוכחה. [א ⇐ ב] אם b שלם, הוא שורש של פולינום מתוקן

$$b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0 = 0$$

עבור $a_0, a_1, \dots, a_{n-1} \in A$. לכן

$$b^n = -a_{n-1} b^{n-1} - \dots - a_1 b - a_0 \in A \cdot b^{n-1} + \dots + A \cdot b + A \cdot 1 = M.$$

מכאן,

$$\begin{aligned} b^{n+1} &= -a_{n-1} b^n - \dots - a_1 b^2 - a_0 b = \\ &= -a_{n-1}\left(-a_{n-1} b^{n-1} - \dots - a_1 b - a_0\right) - \dots - a_1 b^2 - a_0 b \in M \end{aligned}$$

באינדוקציה, לכל $m \in \mathbb{N}$ מתקיים $b^m \in M = A \cdot b^{n-1} + \dots + A \cdot b + A \cdot 1$. לכן נקבל ש-$A[b] = M$ נוצר סופית כ-A-מודול.

[ב ⇐ ג] ניקח $S = A[b]$.

[ג ⇐ ד] ניקח $M = S$. כיוון ש-$1 \in S$, M נאמן.

ד ⇐ א יהי $M = Ax_1 + \cdots + Ax_n$. כיוון ש-$bM \subseteq M$, לכל j מתקיים $bx_j \in M$. לכן קיימים $a_{j,i} \in A$ שעבורם

$$bx_j = \sum_{i=1}^{n} a_{j,i} x_i .$$

נסמן $C = (a_{i,j})$. אזי

$$\begin{pmatrix} bx_1 \\ \vdots \\ bx_n \end{pmatrix} = C \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} ,$$

ובאופן שקול

$$(b \cdot I_n - C) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 .$$

נסמן $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. אזי $(b \cdot I_n - C) x = 0$. נכפול ב-adjoint, ונקבל

$$\det (b \cdot I_n - C) x = \operatorname{adj} (b \cdot I_n - C) \cdot (b \cdot I_n - C) \cdot x = 0 .$$

אבל $\det (b \cdot I_n - C) \in A[b]$, ו-$M$ הוא מודול נאמן מעל $A[b]$. כיוון ש-$\det (b \cdot I_n - C)$ מאפס את היוצרים של M, הוא מאפס את כל M, ולכן $\det (b \cdot I_n - C) = 0$. אבל זהו פולינום מתוקן ב-b, ולכן b שלם מעל A. □

טענה 1.4. יהי A תחום שלמות, ותהי B אלגברה מעל A (לדוגמה, $A \subseteq B$). אזי הסגור השלם של A ב-B הוא חוג.

הוכחה. יהיו $x, y \in B$ שלמים מעל A. קיימים $a_0, a_1, \ldots, a_{n-1}, a'_0, a'_1, \ldots, a'_{m-1} \in A$, לא כולם 0, שעבורם

$$x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$
$$y^m + a'_{m-1} y^{m-1} + \cdots + a'_1 y + a'_0 = 0$$

לכן תת-האלגברה $A[x,y] \subseteq B$ נוצרת מעל A כמודול על ידי

$$\left\{ x^i y^j \mid 0 \le i \le n-1, 0 \le j \le m-1 \right\} ,$$

ובפרט $A[x,y]$ היא A-מודול נוצר סופית. אבל $x + y, x \cdot y \in A[x,y]$. לכן, לפי סעיף ג' של טענה 1.3, $x + y$ ו-$x \cdot y$ שלמים מעל A, כנדרש. □

1.2 שדות מספרים

הגדרה 1.5. שדה מספרים (number field) הינו הרחבה סופית של $\mathbb{Q}$.

דוגמה 1.6. $\mathbb{Q}\left(\sqrt{2}\right)$ ו-$\mathbb{Q}\left(\sqrt[3]{2}\right)$ הם שדות מספרים.

הגדרה 1.7. יהי K שדה מספרים. **חוג השלמים (ring of integers)** של K, שיסומן $\mathcal{O}_K$, הינו הסגור השלם של $\mathbb{Z}$ ב-K.

לפי טענה 1.4, $\mathcal{O}_K$ הינו חוג.

תרגיל 1.8. יהי $K=\mathbb{Q}\left(\sqrt{d}\right)$ עבור $d\neq 0,1$ חופשי מריבועים. אזי

$$\mathcal{O}_K=\begin{cases}\mathbb{Z}\left[\sqrt{d}\right], & d\equiv 2,3 \pmod 4\\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d\equiv 1 \pmod 4\end{cases}.$$

הגדרה 1.9. תהי L/K הרחבה סופית של שדות. נגדיר

$$\Sigma=\left\{\sigma:L\to\overline{K}:\forall x\in K:\sigma(x)=x\right\}.$$

הערה.

א. אם L/K גלואה, $\Sigma=\mathrm{Gal}\left(L/K\right)$.

ב. תמיד $|\Sigma|=[L:K]$.

הגדרה 1.10. יהי $x\in L$. נגדיר את ה**נורמה** (**norm**) ואת ה**עקבה** (**trace**) שלו להיות

$$\mathrm{N}_{L/K}(x)=\prod_{\sigma\in\Sigma}\sigma(x)\in\overline{K}$$
$$\mathrm{Tr}_{L/K}(x)=\sum_{\sigma\in\Sigma}\sigma(x)\in\overline{K}$$

טענה 1.11. יהיו $x,y\in L$.

א. $\mathrm{N}_{L/K}(xy)=\mathrm{N}_{L/K}(x)\cdot\mathrm{N}_{L/K}(y)$ ו-$\mathrm{Tr}_{L/K}(x+y)=\mathrm{Tr}_{L/K}(x)+\mathrm{Tr}_{L/K}(y)$.

ב. $\mathrm{N}_{L/K}(x),\mathrm{Tr}_{L/K}(x)\in K$.

הוכחה.

א. ברור.

ב. נוכיח במקרה ש-L/K גלואה. לכל $\tau\in\mathrm{Gal}\left(L/K\right)$ מתקיים

$$\tau\left(\mathrm{N}_{L/K}(x)\right)=\tau\left(\prod_{\sigma\in\Sigma}\sigma(x)\right)=\prod_{\sigma\in\Sigma}\tau\sigma(x)=\mathrm{N}_{L/K}(x).$$

לכן $\mathrm{N}_{L/K}(x)\in K$. באופן דומה, $\mathrm{Tr}_{L/K}(x)\in K$.

□

דוגמה 1.12. ניקח $K=\mathbb{Q}$ ו-$L=\mathbb{Q}\left(\sqrt{d}\right)$. כל $x\in L$ הוא מהצורה $x=a+b\sqrt{d}$ עבור $a,b\in\mathbb{Q}$. בנוסף, L/K גלואה עם חבורת גלואה שאיבריה הם

$$\sigma_1\left(a+b\sqrt{d}\right)=a+b\sqrt{d},$$
$$\sigma_2\left(a+b\sqrt{d}\right)=a-b\sqrt{d}.$$

אזי

$$\mathrm{N}_{L/K}(x) = \mathrm{N}_{L/K}\left(a+b\sqrt{d}\right) = \left(a+b\sqrt{d}\right)\left(a-b\sqrt{d}\right) = a^2-db^2,$$
$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{L/K}\left(a+b\sqrt{d}\right) = \left(a+b\sqrt{d}\right)+\left(a-b\sqrt{d}\right) = 2a.$$

אם כן, נניח שרוצים למצוא $x,y\in\mathbb{Z}$ שעבורם $x^2-7y^2=1$. אז שקול למצוא $z=x+y\sqrt{7}\in\mathbb{Z}\left[\sqrt{7}\right]$ שעבורו $\mathrm{N}_{\mathbb{Q}(\sqrt{7})/\mathbb{Q}}(z)=1$.

הגדרה 1.13. תחום שלמות A נקרא **סגור בשלמות** (**integrally closed**) אם הוא הסגור השלם של עצמו ב-$\mathrm{Frac}A$.

תרגיל 1.14. סגור שלם תמיד סגור בשלמות.

טענה 1.15. כל תחום פריקות יחידה הוא סגור בשלמות.

הוכחה. יהי A תחום פריקות יחידה, ויהי $x=\frac{\alpha}{\beta}\in\mathrm{Frac}A$ כאשר $\alpha,\beta\in A$ והשבר מצומצם (כיוון ש-A תחום פריקות יחידה, ניתן להציג כך כל איבר של $\mathrm{Frac}A$). נניח ש-x שלם מעל A. אזי קיימים $a_0,a_1,\ldots,a_{n-1}\in A$, לא כולם 0, שעבורם

$$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0.$$

נציב $x=\frac{\alpha}{\beta}$, ונקבל

$$\left(\frac{\alpha}{\beta}\right)^n+a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1}+\cdots+a_1\cdot\frac{\alpha}{\beta}+a_0=0.$$

על ידי הכפלה ב-β^n, נקבל

$$\alpha^n+a_{n-1}\alpha^{n-1}\beta+\cdots+a_1\alpha\beta^{n-1}+a_0\beta^n=0,$$

ועל ידי העברת אגפים

$$\alpha^n=-\left(a_{n-1}\alpha^{n-1}\beta+\cdots+a_1\alpha\beta^{n-1}+\alpha_0\beta^n\right).$$

אגף ימין מתחלק ב-β, ולכן גם אגף שמאל מתחלק ב-β. אבל α ו-β זרים; אילו ל-β היה גורם אי-פריק, אותו גורם היה מחלק את α^n, ולכן גם את α, בסתירה לזרות. לכן $\beta\in A$ הפיך, כלומר $x=\frac{\alpha}{\beta}\in A$. $\square$

מעתה נניח ש-A תחום שלמות סגור בשלמות, $K=\mathrm{Frac}A$, L הרחבה סופית של K ו-B הסגור השלם של A ב-L. כלומר, הדיאגרמה היא כזו:

$$\begin{array}{ccc} B & \subseteq & L \\ \Big| & & \Big| \\ A & \subseteq & K \end{array}$$

טענה 1.16. $\mathrm{N}_{L/K}(B),\mathrm{Tr}_{L/K}(B)\subseteq A$.

הוכחה. יהי $x \in B$. x שלם מעל A, כלומר x הוא שורש של פולינום מתוקן. כל $\sigma(x)$ יהיה גם הוא שורש של אותו פולינום, ולכן כולם שלמים מעל A. בפרט, $\mathrm{N}_{L/K}(x), \mathrm{Tr}_{L/K}(x) \in K$ שלמים מעל A. כיוון ש-A סגור בשלמות, נקבל את הדרוש. □

דוגמה 1.17. $\mathbb{Z}\left[\sqrt{5}\right]$ אינו סגור בשלמות. אכן, $\mathrm{Frac}\mathbb{Z}\left[\sqrt{5}\right] = \mathbb{Q}\left(\sqrt{5}\right)$, אבל האיבר $\frac{1+\sqrt{5}}{2}$ שלם מעל $\mathbb{Z}$, בפרט מעל $\mathbb{Z}\left[\sqrt{5}\right]$, אך אינו שייך ל-$\mathbb{Z}\left[\sqrt{5}\right]$.

תרגיל 1.18. יהי K שדה מספרים, ויהי $x \in \mathcal{O}_K$. אזי $x \in \mathcal{O}_K^*$ אם ורק אם $\mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1$.

1.3 הדיסקרימיננטה

הגדרה 1.19. תהי L/K הרחבה סופית של שדות, ויהי $x_1, x_2, \ldots, x_n \in L$ בסיס של L כמרחב וקטורי מעל K. ה**דיסקרימיננטה (discriminant)** של L מעל K ביחס לבסיס הזה הינה

$$\mathrm{d}_{L/K}(x_1, x_2, \ldots, x_n) = \det\left(\left(\mathrm{Tr}_{L/K}(x_i x_j)\right)\right) \in K.$$

טענה 1.20. יהיו A, B, K, L כנ"ל, ויהי $x \in L$. אזי קיים $0 \neq a \in A$ כך ש-$ax \in B$.

הוכחה. אכן, L אלגברי מעל A, לכן קיימים $a_0, a_1, \ldots, a_n \in A$ (לא כולם 0) שעבורם

$$a_n x^n + \cdots + a_1 x + a_0 = 0.$$

ניתן להניח כי $a_n \neq 0$. נכפול את המשוואה ב-a_n^{n-1}, ונקבל

$$a_n^n x^n + a_{n-1} a_n^{n-1} x^{n-1} + \cdots + a_1 a_n^{n-1} x + a_0 a_n^{n-1} = 0,$$

כלומר

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + a_{n-2} a_n (a_n x)^{n-2} + \cdots + a_0 a_n^{n-1} = 0.$$

הראינו ש-$a_n x$ הוא שורש של פולינום מתוקן מעל A, כלומר $a_n x \in L$ שלם מעל A, ומכאן שייך ל-B. □

מסקנה 1.21. אפשר לבחור בסיס $x_1, \ldots, x_n$ של L מעל K כך ש-$x_i \in B$.

טענה 1.22. יהיו A, B, K, L כנ"ל, יהי $x_1, \ldots, x_n \in B$ בסיס של L מעל K, ותהי

$$d = \mathrm{d}_{L/K}(x_1, \ldots, x_n) \in A$$

הדיסקרימיננטה. אזי

$$d \cdot B \subseteq A \cdot x_1 + \cdots + A \cdot x_n \subseteq B.$$

הוכחה. יהי $b \in B$. בפרט, $b \in L$, ולכן אפשר לכתוב $b = \alpha_1 x_1 + \cdots + \alpha_n x_n$ עבור $\alpha_i \in K$. לכל $1 \leq j \leq n$,

$$\mathrm{Tr}_{L/K}(x_j \cdot b) = \mathrm{Tr}_{L/K}\left(\sum_{i=1}^{n} \alpha_i x_i x_j\right) = \sum_{i=1}^{n} \alpha_i \mathrm{Tr}_{L/K}(x_i x_j).$$

תהי M המטריצה $\left(\mathrm{Tr}_{L/K}(x_i x_j)\right)$, כלומר $d = \det M$. הראינו שמתקיים

$$\begin{pmatrix}\mathrm{Tr}_{L/K}(x_1 \cdot b) & \cdots & \mathrm{Tr}_{L/K}(x_n \cdot b)\end{pmatrix} = \begin{pmatrix}\alpha_1 & \cdots & \alpha_n\end{pmatrix} \cdot M.$$

תהי $\operatorname{adj}(M) \in \mathrm{M}_n(A)$ המטריצה המצורפת של M. אזי $M \cdot \operatorname{adj}(M) = \det M \cdot I = d \cdot I$. אם נכפול את המשוואה שקיבלנו ב-$\operatorname{adj}(M)$ מימין, נקבל

$$\begin{pmatrix} \mathrm{Tr}_{L/K}(x_1 \cdot b) & \cdots & \mathrm{Tr}_{L/K}(x_n \cdot b) \end{pmatrix} \cdot \operatorname{adj}(M) = \begin{pmatrix} d\alpha_1 & \cdots & d\alpha_n \end{pmatrix}.$$

כיוון שכל $\mathrm{Tr}_{L/K}(x_j \cdot b) \in A$, גם אגף ימין יהיה ב-$A$, כלומר $d\alpha_i \in A$ לכל i. בסך הכל,

$$db = d\alpha_1 x_1 + \cdots + d\alpha_n x_n \in A \cdot x_1 + \cdots + A \cdot x_n$$

כנדרש. $\square$

טענה 1.23. תהי L/K הרחבה סופית וספרבילית, ויהי $x_1, \ldots, x_n$ בסיס של L מעל K. אזי

$$\mathrm{d}_{L/K}(x_1, \ldots, x_n) \neq 0.$$

הוכחה. נסמן $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$. אזי

$$\mathrm{Tr}_{L/K}(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j).$$

לכן $M = N^t \cdot N$ עבור $N = (\sigma_i(x_j)) \in \mathrm{M}_n(\overline{K})$. כלומר, בהחלפת בסיס הדיסקרימיננטה מוכפלת בריבוע הדטרמיננטה של מטריצת המעבר מ-N ל-$(\sigma_i(y_j))$. בפרט, אם $d = 0$ ביחס לבסיס אחד, היא תהיה 0 עבור כל בסיס.

לכן מספיק למצוא בסיס כלשהו $y_1, \ldots, y_n$ של L מעל K שעבורו $\mathrm{d}_{L/K}(y_1, \ldots, y_n) \neq 0$. אבל L/K הרחבה סופית וספרבילית, לכן $L = K(\theta)$, ואפשר לקחת את הבסיס $1, \theta, \ldots, \theta^{n-1}$. במקרה הזה

$$N = \begin{pmatrix} 1 & \sigma_1(\theta) & \cdots & \sigma_1(\theta)^{n-1} \\ 1 & \sigma_2(\theta) & \cdots & \sigma_2(\theta)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\theta) & \cdots & \sigma_n(\theta)^{n-1} \end{pmatrix}$$

היא מטריצת ונדרמונדה. מכאן

$$\det N = \prod_{i<j} (\sigma_i(\theta) - \sigma_j(\theta)) \neq 0,$$

כלומר

$$\mathrm{d}_{L/K}(1, \theta, \ldots, \theta^{n-1}) = \det(N^t \cdot N) = (\det N)^2 \neq 0$$

כנדרש. $\square$

טענה 1.24. יהיו A, B, K, L כנ"ל, ונניח בנוסף כי A הוא תחום ראשי. אזי B הינו A-מודול חופשי מדרגה $n = [L : K]$.

הוכחה. יהי $x_1, \ldots, x_n \in B$ בסיס של L מעל K. לפי טענה 1.22, $B \subseteq A \cdot \frac{x_1}{d} + \cdots + A \cdot \frac{x_n}{d}$, ו-$A \cdot \frac{x_1}{d} + \cdots + A \cdot \frac{x_n}{d}$ הוא A-מודול נוצר סופית. A תחום ראשי, בפרט נותרי, ולכן B

נוצר סופית כ-A-מודול. בנוסף, ב-B אין פיתול כי הוא משוכן בשדה. לפי משפט המבנה של מודולים נוצרים סופית מעל תחום ראשי, B חופשי כ-A-מודול. נקבל

$$m = \mathrm{rank}_A B \le \mathrm{rank}_A \left(A \cdot \frac{x_1}{d} + \cdots + A \cdot \frac{x_n}{d} \right) = n.$$

יהי $B = Ay_1 + \cdots + Ay_m$. הוכחנו שכל איבר של L הוא מהצורה $\frac{b}{a}$ עבור $b \in B$ ו-$a \in A$. לכן $L = Ky_1 + \cdots + Ky_m$, ומכאן $m = \mathrm{rank}_A B \ge [L : K] = n$. בסך הכל הוכחנו ש-$m = n$, כפי שרצינו. □

תרגיל 1.25. יהי $B \subseteq M \subseteq L$ נוצר סופית כ-B-מודול. אזי M חופשי מדרגה $[L : K] = n$ כ-A-מודול.

מסקנה 1.26. יהי K שדה מספרים. אזי $\mathcal{O}_K$ הינו $\mathbb{Z}$-מודול חופשי מדרגה $[K : \mathbb{Q}]$. בסיס של $\mathcal{O}_K$ כ-$\mathbb{Z}$-מודול נקרא **בסיס שלם** (***integral basis***) של K.

2 תחומי דדקינד

הגדרה 2.1. חוג קומוטטיבי A נקרא **תחום דדקינד** (**Dedekind domain**) אם הוא תחום שלמות נותרי סגור בשלמות עם מימד קרול 1.

הערה. תחום שלמות הוא בעל מימד קרול 1 אם ורק אם כל אידאל ראשוני לא אפסי הוא מקסימלי.

טענה 2.2. לכל שדה מספרים K, חוג השלמים $\mathcal{O}_K$ הינו תחום דדקינד.

הוכחה. $\mathcal{O}_K \subseteq K$, ולכן $\mathcal{O}_K$ תחום שלמות. כמו כן, $\mathcal{O}_K$ הוא הסגור השלם של $\mathbb{Z}$ ב-K, ולכן הוא סגור בשלמות.

אם נכתוב $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, נקבל אפימורפיזם של חוגים $\mathbb{Z}[x_1, \ldots, x_n] \twoheadrightarrow \mathcal{O}_K$ הנתון על ידי $x_i \mapsto \alpha_i$. $\mathbb{Z}[x_1, \ldots, x_n]$ נותרי לפי משפט הבסיס של הילברט, ומנה של חוג נותרי היא נותרית. לכן $\mathcal{O}_K$ נותרי.

נותר להוכיח שמימד קרול של $\mathcal{O}_K$ הוא 1. יהי $0 \neq P \subseteq \mathcal{O}_K$ אידאל ראשוני. אזי $P \cap \mathbb{Z}$ אידאל ראשוני של $\mathbb{Z}$. נראה שהוא שונה מ-0: יהי $0 \neq y \in P$. לכן אפשר למצוא $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}$, לא כולם 0, שעבורם

$$\underbrace{y^m + a_{m-1}y^{m-1} + \cdots + a_1 y}_{\in P} + a_0 = 0.$$

אפשר להניח כי $a_0 \neq 0$ (כי $\mathcal{O}_K$ תחום שלמות), ולכן $a_0 \in P \cap \mathbb{Z}$. בפרט $P \cap \mathbb{Z} \neq 0$. לכן $P \cap \mathbb{Z} = p\mathbb{Z}$ לאיזשהו מספר ראשוני p.

נניח בשלילה ש-P אינו מקסימלי. $\mathcal{O}_K$ נותרי, ולכן $P \subsetneq Q$ עבור Q מקסימלי. $\mathcal{O}_K/\mathbb{Z}$ הרחבה שלמה, לכן מקיימת Going Down, כלומר

$$p\mathbb{Z} = P \cap \mathbb{Z} \subsetneq Q \cap \mathbb{Z}.$$

אבל $p\mathbb{Z}$ מקסימלי ב-$\mathbb{Z}$, בסתירה. □

2.1 פירוק אידאלים בתחום דדקינד

טענה 2.3. יהי A חוג קומוטטיבי נותרי, ויהי $0 \neq I \subseteq A$ אידאל. אזי קיימים $P_1,\dots,P_r \neq 0$ אידאלים ראשוניים שעבורם $P_1 \dots P_r \subseteq I$.

הוכחה. נוכיח את הטענה באינדוקציה נותרית. תהי $\mathcal{I}$ קבוצת האידאלים של A שאינם מקיימים את המשפט. אם $\mathcal{I} \neq \varnothing$, מהנותריות קיים I מקסימלי ב-$\mathcal{I}$. ברור כי I אינו ראשוני, ולכן קיימים $a,b \notin I$ שעבורם $a \cdot b \in I$.

נגדיר $J_1 = I + aA$ ו-$J_2 = I + bA$. מהמקסימליות, אפשר למצוא אידאלים ראשוניים שעבורם

$$P_1 \dots P_r \subseteq J_1, \qquad Q_1 \dots Q_s \subseteq J_2.$$

לכן $P_1 \dots P_r Q_1 \dots Q_r \subseteq J_1 J_2 \subseteq I$, בסתירה. □

טענה 2.4. יהי A תחום דדקינד, יהי $K = \mathrm{Frac}A$, ויהי I אידאל אמיתי של A. אזי קיים $x \in K \setminus A$ כך ש-$xI \subseteq A$.

הוכחה. אם $I = 0$, המשפט טריוויאלי; לכן נניח $I \neq 0$. נקבע $0 \neq y \in I$. לפי הטענה הקודמת, קיימים אידאלים ראשוניים $P_1,\dots,P_r$ שעבורם

$$P_1 \dots P_r \subseteq yA \subseteq I.$$

נבחר r מינימלי כנ"ל. יהי P אידאל מקסימלי, לכן ראשוני, המכיל את I. אזי קיים i שעבורו $P_i \subseteq P$. אבל P_i גם הוא מקסימלי, לכן $P_i = P$. בלי הגבלת הכלליות, $P = P_r$. מהמינימליות של r, $P_1 \dots P_{r-1} \not\subseteq yA$; נבחר $b \in P_1 \dots P_{r-1} \setminus yA$, וניקח $x = \frac{b}{y}$. אזי

$$xyI = bI \subseteq P_1 \dots P_{r-1} \subseteq yA$$

ומכאן $xI \subseteq A$, כנדרש. □

הגדרה 2.5. יהי A תחום דדקינד, יהי $K = \mathrm{Frac}A$, ויהי $I \subseteq A$ אידאל לא אפסי. נגדיר

$$I^{-1} = \{x \in K \mid xI \subseteq A\}$$

מהטענה הקודמת, $I^{-1} \not\subseteq A$.

טענה 2.6. יהי $P \subseteq A$ אידאל ראשוני לא אפסי. אזי $PP^{-1} = A$.

הוכחה. לפי הגדרת P, $PP^{-1} \subseteq A$. כיוון ש-$1 \in P^{-1}$, $P \subseteq PP^{-1} \subseteq A$. מצד שני, PP^{-1} הוא אידאל של A. אבל P מקסימלי, לכן $PP^{-1} = A$ או $PP^{-1} = P$.

נניח בשלילה כי $PP^{-1} = P$. מטענה 2.4, קיים $x \in P^{-1} \setminus A$. באופן טבעי, P הינו $A[x]$-מודול, כי $xP \subseteq PP^{-1} = P$. אבל P נוצר סופית כ-A-מודול, ו-P נאמן כ-$A[x]$-מודול (כי הוא מוכל בתחום שלמות), ולכן לפי סעיף ד' של טענה 1.3 x שלם מעל A. אבל A סגור בשלמות, לכן $x \in A$, בסתירה. מכאן בהכרח $PP^{-1} = A$. □

משפט 2.7. יהי A תחום דדקינד, ויהי $I \subseteq A$ אידאל לא אפסי. אזי אפשר לבטא את I באופן יחיד כמכפלה של אידאלים ראשוניים של A.

הוכחה.

קיום. נניח בשלילה שלא. תהי $\mathcal{S}$ קבוצת האידאלים של A שאינם מכפלה של אידאלים ראשוניים; לכן $\mathcal{S} \neq \varnothing$. כיוון ש-$A$ נותרי, קיים I מקסימלי ביחס לתכונה הזו. I אינו ראשוני, בפרט אינו מקסימלי, ולכן קיים P מקסימלי כך ש-$I \subsetneq P$.

טענה. $IP^{-1} \subsetneq A$.

הוכחה. יהי $x \in P \setminus I$. אם בשלילה $PP^{-1} = A = IP^{-1}$, אזי $xP^{-1} \subseteq PP^{-1} = IP^{-1}$. לכן מתקיים $xA = xP^{-1}P \subseteq IP^{-1}P = IA = I$, בסתירה לכך ש-$x \notin I$. □

טענה. $IP^{-1} \supsetneq I$.

הוכחה. יהי $x \in P^{-1} \setminus A$. אם נניח בשלילה ש-$IP^{-1} = I$, אזי I הינו $A[x]$-מודול (נאמן). אבל I נוצר סופית כ-A-מודול, לכן x שלם מעל A. כיוון ש-A סגור בשלמות, $x \in A$, בסתירה. □

משתי הטענות האלו, $IP^{-1} \notin \mathcal{S}$ (מהמקסימליות של I). לכן

$$I = IA = IP^{-1}P = P_1 \ldots P_r P$$

בסתירה לכך ש-$I \in \mathcal{S}$. לכן $\mathcal{S} = \varnothing$.

יחידות. נניח $I = P_1 \ldots P_r = Q_1 \ldots Q_s$. בפרט מתקיים $P_1 \ldots P_r \subseteq Q_s$. Q_s ראשוני, לכן קיים i שעבורו $P_i \subseteq Q_s$. בלי הגבלת הכלליות, $P_r \subseteq Q_s$. כיוון שמימד קרול של A הוא 1, שני האידאלים מקסימליים, ולכן $P_r = Q_s$. נקבל

$$IP_r^{-1} = P_1 \ldots P_{r-1} = Q_1 \ldots Q_{s-1}$$

ומכאן נסיים באינדוקציה.

□

2.2 אידאלים שבריים וחבורת המחלקות

הגדרה 2.8. יהי A תחום דדקינד, ויהי $K = \mathrm{Frac}A$. **אידאל שברי (fractional ideal)** של A הינו תת-A-מודול של K שנוצר סופית מעל A. נסמן על ידי $\mathcal{J}_A$ את קבוצת האידאלים השבריים של A.

הערה. מעתה, לאידאלים "רגילים" של A נקרא **אידאלים שלמים**.

טענה 2.9. $\mathcal{J}_A$ חבורה אבלית תחת הפעולה

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_{i=1}^{n} x_i y_i : x_i \in \mathfrak{a}, y_i \in \mathfrak{b} \right\}.$$

הוכחה. הסגירות והאסוציאטיביות ברורות, ואיבר היחידה הוא A. נותר רק לבדוק את קיום ההופכיים.

אם I אידאל שלם של A, $I = P_1 \ldots P_r$, ואז $I^{-1} = P_1^{-1} \ldots P_r^{-1}$.

נוודא שכל P^{-1} נוצר סופית. אכן, P נוצר סופית מהנותריות של A. לכן אפשר לכתוב $P = Ay_1 + \cdots + Ay_m$. אם $x \in P^{-1}$, אזי $xy_i \in A$ לכל $1 \leq i \leq m$. בפרט, $x \in \frac{1}{y_1}A$; לכן גם $P^{-1} \subseteq \frac{1}{y_1}A$. אבל A נותרי, ולכן P^{-1} נוצר סופית. מכאן שגם I^{-1} נוצר סופית.

הוכחנו שלכל אידאל שלם יש הופכי. כעת, יהי $\mathfrak{a} \in \mathcal{J}_A$ אידאל שברי. אפשר לכתוב $\mathfrak{a} = Ay_1 + \cdots + Ay_m$. כל $y_i \in K$, לכן אפשר לכתוב $y_i = \frac{a_i}{b_i}$ לאילושהם $a_i, b_i \in K$. יהי $b = b_1 \ldots b_m$. אזי $b\mathfrak{a} \subseteq A$, כי $by_i \in A$ לכל $1 \leq i \leq m$; לכן $b\mathfrak{a}$ הינו אידאל שלם, ונוכל לקחת $\mathfrak{a}^{-1} = b \cdot I^{-1}$. □

הגדרה 2.10. תהי $\mathcal{P}_A \subseteq \mathcal{J}_A$ תת-החבורה המכילה את האידאלים השבריים הראשיים xA עבור כל $x \in K$. המנה $\mathrm{Cl}_A = \mathcal{J}_A/\mathcal{P}_A$ נקראת **חבורת המחלקות** (**ideal class group**) של A.

הערה. A תחום ראשי אם ורק אם $\mathrm{Cl}_A = \{e\}$.

משפט (*L. Claborn*, 1966)**.** תהי G חבורה אבלית כלשהי. אזי קיים תחום דדקינד A כך ש-$\mathrm{Cl}_A \cong G$.

בשנות ה-70, C. Leedham Green הראה שאפשר אפילו למצוא דוגמה בצורה

$$\begin{array}{ccc} A & \subseteq & K \\ & & \Big|\,{\scriptstyle 2} \\ R & \subseteq & \mathrm{Frac}R \end{array}$$

כאשר R תחום ראשי ו-$[K : \mathrm{Frac}R] = 2$.

מטרה. יהי K שדה מספרים; נסמן $\mathrm{Cl}_K = \mathrm{Cl}_{\mathcal{O}_K}$ ו-$\mathcal{J}_K = \mathcal{J}_{\mathcal{O}_K}$. נרצה להוכיח כי Cl_K היא תמיד חבורה סופית.

2.3 הנורמה של אידאל

הגדרה 2.11. יהי A תחום דדקינד, ויהיו $I, J \subseteq A$ אידאלים. אזי $I \mid J$ אם קיים אידאל I' כך ש-$J = II'$.

תרגיל. $I \mid J$ אם ורק אם $J \subseteq I$.

הגדרה 2.12. יהי K שדה מספרים, ויהי $I \subseteq \mathcal{O}_K$ אידאל. **הנורמה** (**ideal norm**) של I הינה

$$\mathrm{N}(I) = \begin{cases} |\mathcal{O}_K/I|, & I \neq 0 \\ 0, & I = 0 \end{cases}.$$

טענה 2.13. יהיו $I, J \subseteq \mathcal{O}_K$ אידאלים. אזי $\mathrm{N}(IJ) = \mathrm{N}(I) \cdot \mathrm{N}(J)$.

הוכחה. אם I ו-J זרים, $I + J = \mathcal{O}_K$. לפי משפט השאריות הסיני,

$$\mathcal{O}_K/IJ \cong \mathcal{O}_K/I \times \mathcal{O}_K/J.$$

זה מראה ש-$\mathrm{N}(IJ) = \mathrm{N}(I) \cdot \mathrm{N}(J)$ במקרה ש-I ו-J זרים. לכן מספיק להוכיח את הטענה במקרה ש-$I = P^n$ ו-$J = P^m$ עבור אידאל ראשוני P.

טענה. לכל $n \geq 1$, $\mathcal{O}_K/P \cong P^n/P^{n+1}$.

הוכחה. יהי $x \in P^n \setminus P^{n+1}$ (קיים מיחידות הפירוק לראשוניים). נגדיר

$$\varphi : \mathcal{O}_K \to P^n/P^{n+1}$$
$$a \mapsto ax + P^{n+1}$$

נראה ש-$\ker\varphi = P$. אכן, $P \subseteq \ker\varphi$. יהי $a \in \ker\varphi$; אזי $ax \in P^{n+1}$, כלומר

$$ax\mathcal{O}_K = (a\mathcal{O}_K)(x\mathcal{O}_K) \subseteq P^{n+1}.$$

אם כן, $P^{n+1} \mid ax\mathcal{O}_K$, כלומר $(a\mathcal{O}_K)(x\mathcal{O}_K) = P^{n+1} \cdot I$. אבל P מופיע בדיוק n פעמים בפירוק של $x\mathcal{O}_K$, לכן הוא מופיע בפירוק של $a\mathcal{O}_K$, כלומר $a\mathcal{O}_K \subseteq P$, ובפרט $a \in P$.

כעת נוכיח ש-φ על. יהי $y \in P^n$. $x \in P^n \setminus P^{n+1}$, לכן $x\mathcal{O}_K = P^n J$ כאשר J זר ל-P. לפי משפט השאריות הסיני, קיים $b \in \mathcal{O}_K$ כך ש-$b \equiv 0 \pmod J$ וגם $b \equiv y \pmod{P^{n+1}}$. אם כן, $b \in P^n$ וגם $b \in J$, ולכן $x\mathcal{O}_K = P^n J \mid b\mathcal{O}_K$. מכאן $b \in b\mathcal{O}_K \subseteq x\mathcal{O}_K$, כלומר $b = xa$ לאיזשהו $a \in \mathcal{O}_K$, ואז $\varphi(a) = b + P^{n+1} = y + P^{n+1}$. זה מוכיח ש-$\varphi$ על. □

באינדוקציה, נקבל כי $\mathrm{N}(P^m) = \mathrm{N}(P)^m$; זה מוכיח את הכפליות לחזקות של אידאל ראשוני, ולכן סיימנו. □

טענה 2.14. יהי $I \subseteq \mathcal{O}_K$ אידאל. אזי $\mathrm{N}(I) < \infty$.

הוכחה. אפשר להניח $I \neq 0$.

טענה. יהי $P \subseteq \mathcal{O}_K$ אידאל ראשוני. אזי $\mathrm{N}(P) < \infty$.

הוכחה. לפי משפט שהוכחנו, $\mathcal{O}_K$ הוא $\mathbb{Z}$-מודול חופשי מדרגה $n = [K:\mathbb{Q}]$, כלומר

$$\mathcal{O}_K = \mathbb{Z}c_1 + \cdots + \mathbb{Z}c_n.$$

P ראשוני, ומכאן ש-$P \cap \mathbb{Z} = p\mathbb{Z}$ לאיזשהו מספר ראשוני p. לכן

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_p c_1 + \cdots + \mathbb{F}_p c_n$$

היא מנה סופית. כיוון ש-$p\mathcal{O}_K \subseteq P$, יש הטלה $\mathcal{O}_K/p\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/P$, ובפרט $\mathcal{O}_K/P$ סופי. □

הסופיות של הנורמה עבור I נובעת מהפירוק של כל אידאל למכפלה של ראשוניים ומכפליות הנורמה. □

טענה 2.15. יהי M מספר טבעי. אזי יש מספר סופי של אידאלים $I \subseteq \mathcal{O}_K$ כך ש-$\mathrm{N}(I) \leq M$.

הוכחה. מספיק להוכיח שיש רק מספר סופי של אידאלים ראשוניים P עם $\mathrm{N}(P) \leq M$, שהרי $\mathrm{N}(P) > 1$. אבל כבר הוכחנו שאם $P \cap \mathbb{Z} = p\mathbb{Z}$, אזי $\mathrm{N}(P)$ הינה חזקה של p. בפרט, $\mathrm{N}(P) \geq p$. הטענה נובעת מכך שיש מספר סופי של ראשוניים $p \leq M$, ומכך שיש מספר סופי של אידאלים ראשוניים $P \subseteq \mathcal{O}_K$ המקיימים $P \mid p\mathcal{O}_K$. □

ניזכר שברצוננו להוכיח כי Cl_K היא חבורה סופית. לפי טענה 2.15, מספיק למצוא M טבעי כך שכל אידאל של $\mathcal{O}_K$ שקול (מודולו $\mathcal{P}_K = \mathcal{P}_{\mathcal{O}_K}$) לאידאל עם נורמה שחסומה על ידי M. בשביל להוכיח זאת, נפתח מעט כלים על שריגים.

2.4 שריגים

הגדרה 2.16. יהי $V=\mathbb{R}^n$ מרחב וקטורי מעל $\mathbb{R}$. **שריג (lattice)** הינו

$$\Gamma=\mathbb{Z}v_1+\mathbb{Z}v_2+\cdots+\mathbb{Z}v_m\subseteq V$$

כך ש-$v_1,\ldots,v_m$ בלתי-תלויים מעל $\mathbb{R}$. Γ נקרא **שלם (complete)** אם $m=n$.

הגדרה 2.17. תת-חבורה $\Gamma\subseteq V$ נקראת **דיסקרטית (discrete)** אם לכל $\gamma\in\Gamma$ קיימת קבוצה פתוחה $U\subseteq V$ כך ש-$U\cap\Gamma=\{\gamma\}$.

טענה 2.18. תהי $\Gamma\subseteq V$ תת-חבורה. אזי Γ שריג אם ורק אם Γ דיסקרטית.

הוכחה. $\boxed{\Leftarrow}$ נכתוב $\Gamma=\mathbb{Z}v_1+\mathbb{Z}v_2+\cdots+\mathbb{Z}v_m$, ונשלים את $v_1,\ldots,v_m$ לבסיס $v_1,\ldots,v_n$ של V. אם $\gamma=b_1v_1+\cdots+b_mv_m$, ניקח

$$U_\gamma=\left\{a_1v_1+\cdots+a_nv_n:|a_i-b_i|<\frac{1}{2}\right\}.$$

אזי U_γ קבוצה פתוחה המקיימת $U_\gamma\cap\Gamma=\{\gamma\}$.

$\boxed{\Rightarrow}$ נחלק את ההוכחה למספר צעדים.

צעד 1. נוכיח כי Γ סגורה.
תהי U פתוחה כך ש-$U\cap\Gamma=\{0\}$. קיים $\varepsilon>0$ כך ש-$B_\varepsilon(0)\subseteq U$. תהי $\{\gamma_n\}$ סדרה מתכנסת של איברים מ-Γ. זה אומר שקיים N כך שלכל $m,n\geq N$,

$$|\gamma_n-\gamma_m|<\varepsilon\Rightarrow\gamma_n-\gamma_m\in B_\varepsilon(0)\subseteq U\cap\Gamma\Rightarrow\gamma_n-\gamma_m=0,$$

כלומר הסדרה $\{\gamma_n\}$ מתייצבת, ובפרט הגבול ב-Γ. לכן Γ סגורה.

יהי $V_0\subseteq V$ תת-המרחב הנפרש על ידי Γ, ויהי $u_1,\ldots,u_m$ בסיס של V_0 כך ש-$u_i\in\Gamma$ לכל $1\leq i\leq m$. נגדיר $\Gamma_0=\mathbb{Z}u_1+\cdots+\mathbb{Z}u_m$.

צעד 2. נראה כי האינדקס $[\Gamma:\Gamma_0]$ סופי.
תהי $\{\gamma_i:i\in I\}$ קבוצת נציגים של הקוסטים ב-Γ/Γ_0, ויהי

$$\Phi_0=\{a_1u_1+\cdots+a_mu_m:0\leq a_i<1\}.$$

אזי $V_0=\bigcup_{\delta\in\Gamma_0}(\Phi_0+\delta)$, והאיחוד זר.
כל $\gamma_i\in\Gamma\subseteq V_0$, לכן $\gamma_i=\mu_i+\delta_i$ באופן יחיד כאשר $\delta_i\in\Gamma_0$ ו-$\mu_i\in\Phi_0$. אבל $\mu_i=\gamma_i-\delta_i\in\Gamma$, לכן $\mu_i\in\overline{\Phi_0}\cap\Gamma$ כש-$\overline{\Phi_0}\cap\Gamma$ קומפקטית ודיסקרטית, ובפרט סופית.
אם כן, יש מספר סופי של אופציות עבור μ_i; אבל $\gamma_i\equiv\mu_i\pmod{\Gamma_0}$, מה שמוכיח את הטענה.

צעד 3. נסיק כי Γ שריג.
אכן, יהי $d=[\Gamma:\Gamma_0]$. $d\Gamma\subseteq\Gamma_0$, כלומר $\Gamma\subseteq\frac{1}{d}\Gamma_0=\mathbb{Z}\frac{u_1}{d}+\cdots+\mathbb{Z}\frac{u_m}{d}$. לפי המיון של חבורות אבליות נוצרות סופית, אפשר לכתוב $\Gamma=\mathbb{Z}v_1+\cdots+\mathbb{Z}v_r$ כאשר $r\leq m$. אבל Γ פורש את V_0 מעל $\mathbb{R}$, לכן $r=m$ והווקטורים $v_1,\ldots,v_r$ בלתי-תלויים לינארית.

□

טענה 2.19. יהי $\Gamma \subseteq V$ שריג. אזי Γ שריג שלם אם ורק אם קיימת קבוצה חסומה $B \subseteq V$ שעבורה $V = \bigcup_{\gamma\in\Gamma}(B+\gamma)$.

הוכחה. $\boxed{\Leftarrow}$ אם $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ שריג שלם כאשר $v_1, \ldots, v_n$ בסיס של V, אז ניקח

$$B = \{a_1v_1 + \cdots + a_nv_n : 0 \le a_i \le 1\}.$$

$\boxed{\Rightarrow}$ יהי V_0 תת-המרחב הנפרש על ידי Γ. מספיק להוכיח כי $V_0 = V$. יהי $v \in V$; כיוון ש-$V = \bigcup_{\gamma\in\Gamma}(B+\gamma)$, לכל $m \ge 1$ אפשר לכתוב $mv = \beta_m + \gamma_m$ עבור $\beta_m \in B$ ו-$\gamma_m \in \Gamma \subseteq V_0$. על ידי חלוקה ב-$m$, נקבל

$$v = \frac{1}{m}\beta_m + \frac{1}{m}\gamma_m.$$

אם נשאיף $m \to \infty$, $\frac{1}{m}\beta_m \to 0$ (כי B חסומה); לכן,

$$V_0 \ni \frac{1}{m}\gamma_m \to v.$$

כיוון ש-V_0 סגור, $v \in V_0$. לכן $V = V_0$, כנדרש. □

הגדרה 2.20. תהי $X \subseteq \mathbb{R}^n$ תת-קבוצה.

א. X נקראת **סימטרית** (**symmetric**) אם לכל $x \in X$, גם $-x \in X$.

ב. X נקראת **קמורה** (**convex**) אם לכל $x_1, x_2 \in X$ מתקיים ש-$tx_1 + (1-t)x_2 \in X$ לכל $t \in [0,1]$.

הגדרה 2.21. עבור שריג $\Gamma \subseteq V$ נסמן $\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi)$, כאשר Φ תחום יסודי של Γ, כלומר

$$V_0 = \mathrm{Span}_{\mathbb{R}}\Gamma = \bigcup_{\gamma\in\Gamma}(\Phi+\gamma)$$

והאיחוד זר.

טענה 2.22 (חסם מינקובסקי). יהי $\Gamma \subseteq V = \mathbb{R}^n$ שריג שלם, תהי $X \subseteq V$ קבוצה סימטרית וקמורה, ונניח $\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma)$. אזי קיים $0 \ne \gamma \in \Gamma$ כך ש-$\gamma \in X$.

הוכחה. מספיק להוכיח שהקבוצות $\left\{\frac{1}{2}X + \gamma\right\}_{\gamma\in\Gamma}$ אינן זרות; אכן, אם

$$y \in \left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right)$$

עם $\gamma_1 \ne \gamma_2$, נכתוב

$$\frac{1}{2}x_1 + \gamma_1 = y = \frac{1}{2}x_2 + \gamma_2.$$

אזי

$$\Gamma \ni \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1 = \frac{1}{2}x_2 + \frac{1}{2}(-x_1) \in X$$

מהסימטריה ומהקמירות.

לכן, נניח בשלילה שהקבוצות כן זרות. בפרט, גם $\left\{\Phi\cap\left(\frac{1}{2}X+\gamma\right)\right\}_{\gamma\in\Gamma}$ זרות זו לזו. נקבל שמתקיים

$$\operatorname{vol}\left(\Gamma\right)=\operatorname{vol}\left(\Phi\right)\geq\sum_{\gamma\in\Gamma}\operatorname{vol}\left(\Phi\cap\left(\frac{1}{2}X+\gamma\right)\right)=\sum_{\gamma\in\Gamma}\operatorname{vol}\left(\frac{1}{2}X\cap\left(\Phi-\gamma\right)\right)=(\star)$$

האיחוד של הקבוצות האלו מכיל את $\frac{1}{2}X$, ולכן

$$(\star)\geq\operatorname{vol}\left(\frac{1}{2}X\right)=\left(\frac{1}{2}\right)^{n}\operatorname{vol}\left(X\right)$$

בסתירה להנחה ש-$\operatorname{vol}\left(X\right)>2^{n}\operatorname{vol}\left(\Gamma\right)$. $\square$

2.5 חסם מינקובסקי ומספר המחלקות

הערה. כל מחלקה של Cl_{K} מכילה אידאל שלם.

אכן, יהי $\mathfrak{a}\in\mathcal{J}_{K}$ אידאל שברי. נכתוב $\mathfrak{a}=P_{1}^{e_{1}}\dots P_{r}^{e_{r}}$ כאשר $P_{1},\dots,P_{r}\subseteq\mathcal{O}_{K}$ אידאלים ראשוניים ו-$e_{1},\dots,e_{r}\in\mathbb{Z}$. אז אפשר לכתוב

$$\mathfrak{a}=P_{1}^{e_{1}}\dots P_{s}^{e_{s}}\left(Q_{1}^{f_{1}}\dots Q_{t}^{f_{t}}\right)^{-1}$$

כאשר $e_{i},f_{i}>0$. יהי $0\neq x\in Q_{1}^{f_{1}}\dots Q_{t}^{f_{t}}$. לכן $x\mathcal{O}_{K}\subseteq Q_{1}^{f_{1}}\dots Q_{t}^{f_{t}}$. מכאן שאפשר לכתוב $x\mathcal{O}_{K}=Q_{1}^{f_{1}}\dots Q_{t}^{f_{t}}I$ לאיזשהו אידאל $I\subseteq\mathcal{O}_{K}$. נקבל

$$\mathfrak{a}\cdot\left(x\mathcal{O}_{K}\right)=\mathfrak{a}\cdot Q_{1}^{f_{1}}\dots Q_{t}^{f_{t}}I=P_{1}^{e_{1}}\dots P_{s}^{e_{s}}I$$

וזהו אידאל שלם השייך למחלקה של $\mathfrak{a}$.

משפט 2.23 (חסם מינקובסקי). יהי K שדה מספרים, $n=\left[K:\mathbb{Q}\right]$. יהי r מספר השיכונים הממשיים $K\hookrightarrow\mathbb{R}$, ויהי s מספר זוגות השיכונים המרוכבים (עד כדי הצמדה) $K\hookrightarrow\mathbb{C}$. בפרט, $r+2s=n$. אז בכל מחלקה של Cl_{K} יש אידאל שלם $I\subseteq\mathcal{O}_{K}$ המקיים

$$\mathrm{N}\left(I\right)\leq\frac{n!}{n^{n}}\cdot\left(\frac{4}{\pi}\right)^{s}\cdot\sqrt{\left|d_{K}\right|}.$$

הוכחה. תהי $C\in\mathrm{Cl}_{K}$ מחלקה, ויהי $J\in C^{-1}$ אידאל שלם. ל-J עשויה להיות נורמה עצומה, אבל אנחנו נשתמש בו על מנת לייצר אידאל באותה מחלקה ומנורמה חסומה.

יהי $\alpha_{1},\dots,\alpha_{n}$ בסיס שלם של K, כלומר $\mathcal{O}_{K}=\mathbb{Z}\alpha_{1}+\dots+\mathbb{Z}\alpha_{n}$. לכן קיימים $\beta_{1},\dots,\beta_{n}\in J$ כך ש-$J=\mathbb{Z}\beta_{1}+\dots+\mathbb{Z}\beta_{n}$. יהיו $\sigma_{1},\dots,\sigma_{r}:K\hookrightarrow\mathbb{R}$ כל השיכונים הממשיים, ויהיו $\tau_{1},\overline{\tau_{1}},\dots,\tau_{s},\overline{\tau_{s}}:K\hookrightarrow\mathbb{C}$ כל השיכונים המרוכבים. נגדיר שיכון $\iota:K\hookrightarrow\mathbb{R}^{n}$ לפי

$$x\mapsto\left(\sigma_{1}\left(x\right),\dots,\sigma_{r}\left(x\right),\operatorname{Re}\tau_{1}\left(x\right),\operatorname{Im}\tau_{1}\left(x\right),\dots,\operatorname{Re}\tau_{s}\left(x\right),\operatorname{Im}\tau_{s}\left(x\right)\right).$$

זה שיכון של חבורות אבליות.

תהי $B\in\mathrm{M}_{n}\left(\mathbb{R}\right)$ המטריצה ששורותיה הן $\iota\left(\beta_{i}\right)$. נחשב את הדטרמיננטה שלה.

תהי

$$M=\begin{pmatrix}\sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1}(\alpha_1) & \cdots & \tau_s(\alpha_1) & \overline{\tau_s}(\alpha_1)\\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau_1}(\alpha_n) & \cdots & \tau_s(\alpha_n) & \overline{\tau_s}(\alpha_n)\end{pmatrix}\in \mathrm{M}_n(\mathbb{R}).$$

אזי $M^tM=\left(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)$, ולכן $|\mathrm{d}_K|=|\det M|^2$, כלומר $|\det M|=\sqrt{|\mathrm{d}_K|}$.
תהי $A\in\mathrm{M}_n(\mathbb{R})$ המטריצה ששורותיה הן $\iota(\alpha_i)$. אזי

$$A=\begin{pmatrix}\sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \operatorname{Re}\tau_1(\alpha_1) & \cdots & \operatorname{Im}\tau_s(\alpha_1)\\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots\\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}\tau_1(\alpha_n) & \cdots & \operatorname{Im}\tau_s(\alpha_n)\end{pmatrix}=$$

$$=M\cdot\left(\begin{array}{ccc|ccc}1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ \hline & & & \frac{1}{2} & \frac{1}{2i} & \\ & & & \frac{1}{2} & -\frac{1}{2i} & \\ & & & & & \ddots\end{array}\right).$$

לכן

$$|\det A|=\frac{1}{2^s}\sqrt{|\mathrm{d}_K|}.$$

נכתוב $\beta_i=\sum_{j=1}^n c_{i,j}\alpha_j$, $c_{i,j}\in\mathbb{Z}$. אם $C=(c_{i,j})$, ו $B=CA^t$, כאשר $|\det C|=\mathrm{N}(J)$. בנוסף,

$$|\det B|=\left(\frac{1}{2}\right)^s\mathrm{N}(J)\sqrt{|\mathrm{d}_K|}.$$

התמונה $\Gamma=\iota(J)$ של $\iota:K\to\mathbb{R}^n$ הינה השריג הנפרש מעל $\mathbb{Z}$ על ידי $\iota(\beta_1),\ldots,\iota(\beta_n)$.
אם כן,

$$\mathrm{vol}(\Gamma)=\left(\frac{1}{2}\right)^s\mathrm{N}(J)\sqrt{|\mathrm{d}_K|}.$$

לכל $t>0$ נגדיר את הקבוצה

$$X_t=\left\{(x_1,\ldots,x_r,y_{11},y_{12},\ldots,y_{s1},y_{s2})\in\mathbb{R}^n : |x_1|+\cdots+|x_r|+2\sqrt{y_{11}^2+y_{12}^2}+\cdots+2\sqrt{y_{s1}^2+y_{s2}^2}<t\right\}.$$

הקבוצה X_t היא סימטרית, קמורה ומקיימת $\mathrm{vol}(X_t)=\frac{2^{r-s}\pi^s t^n}{n!}$. נבחר t המקיים

$$2^n\cdot\mathrm{vol}(\Gamma)<\mathrm{vol}(X_t)<2^n\cdot\mathrm{vol}(\Gamma)+\varepsilon.$$

לפי טענה 2.22, קיים איבר $0\neq\gamma\in\Gamma\cap X_t$. אבל $\Gamma=\iota(J)$, כלומר $\gamma=\iota(u)$ עבור $u\in J$. לכן

$$\begin{aligned}\left|\mathrm{N}_{K/\mathbb{Q}}(u)\right|^{1/n}&=|\sigma_1(u)\ldots\sigma_r(u)\tau_1(u)\overline{\tau_1}(u)\ldots\tau_s(u)\overline{\tau_s}(u)|^{1/n}\leq\\ &\leq\frac{1}{n}\left(|\sigma_1(u)|+\cdots+|\sigma_r(u)|+2|\tau_1(u)|+\cdots+2|\tau_s(u)|\right)=\\ &=\frac{1}{n}\left(|\sigma_1(u)|+\cdots+|\sigma_r(u)|+2\sqrt{(\operatorname{Re}\tau_1(u))^2+(\operatorname{Im}\tau_1(u))^2}+\cdots\right)<\frac{1}{n}\cdot t\end{aligned}$$

כשאי-השוויון האחרון נובע מכך ש-$\iota(u) \in X_t$. זה אומר שמתקיים

$$\mathrm{N}(u\mathcal{O}_K) = \left|\mathrm{N}_{K/\mathbb{Q}}(u)\right| < \frac{t^n}{n^n}.$$

אבל $2^n \cdot \mathrm{vol}(\Gamma) < \mathrm{vol}(X_t)\, 2^n \cdot \mathrm{vol}(\Gamma) + \varepsilon$, לכן

$$2^{r+s}\mathrm{N}(J)\sqrt{|\mathrm{d}_K|} < \frac{2^{r-s}\pi^s t^n}{n!} < 2^{r+s}\mathrm{N}(J)\sqrt{|\mathrm{d}_K|} + \varepsilon$$

כלומר

$$\frac{2^{2s}\mathrm{N}(J)\sqrt{|\mathrm{d}_K|}n!}{\pi^s} < t^n < \frac{2^{2s}\mathrm{N}(J)\sqrt{|\mathrm{d}_K|}n!}{\pi^s} + \frac{n!}{2^{r-s}\pi^s}\varepsilon.$$

אם כן, הראינו שמתקיים

$$\mathrm{N}(u\mathcal{O}_K) \le \left(\frac{4}{\pi}\right)^s \mathrm{N}(J)\frac{n!}{n^n}\sqrt{|\mathrm{d}_K|} + \underbrace{\varepsilon}_{\to 0}.$$

אבל $u \in J$, לכן יש אידאל $I \subseteq \mathcal{O}_K$ שעבורו $u\mathcal{O}_K = IJ$. מכאן שמתקיים

$$\mathrm{N}(I) = \frac{\mathrm{N}(u\mathcal{O}_K)}{\mathrm{N}(J)} \le \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot \sqrt{|\mathrm{d}_K|}.$$

כמו כן, כיוון ש-$I = (u\mathcal{O}_K)J^{-1}$, מתקיים $I \in C$, כפי שרצינו. □

הגדרה 2.24. מספר המחלקות (class number) של K הינו $h_K = |\mathrm{Cl}_K|$.

מסקנה 2.25. $h_K < \infty$.

טענה 2.26. $\mathbb{Z}\left[\sqrt{-1}\right]$ תחום ראשי.

הוכחה. נגדיר $K = \mathbb{Q}\left(\sqrt{-1}\right)$. $-1 \equiv 3 \pmod 4$, ולכן $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-1}\right]$. עבור K הנתון, $n = 2$, $r = 0$ ו-$s = 1$. לפי חסם מינקובסקי, כל מחלקה של Cl_K מכילה אידאל I עם

$$\mathrm{N}(I) \le \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot \sqrt{|\mathrm{d}_K|} = \frac{4}{\pi}\cdot\frac{2}{4}\cdot\sqrt{|-4|} < 2.$$

אבל $\mathrm{N}(I)$ מספר שלם, לכן כל מחלקה מכילה איבר מנורמה 1, כלומר את האיבר הטריוויאלי $\mathcal{O}_K \in \mathcal{J}_K$. מכאן $h_K = 1$, ולכן $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{-1}\right]$ תחום ראשי. □

משפט (*Stark, 1969*)**.** השדות הריבועיים המדומים ($K = \mathbb{Q}\left(\sqrt{-d}\right)$ עבור $d > 0$) עם $h_K = 1$ הם

$$\mathbb{Q}\left(\sqrt{-1}\right), \mathbb{Q}\left(\sqrt{-2}\right), \mathbb{Q}\left(\sqrt{-3}\right), \mathbb{Q}\left(\sqrt{-7}\right), \mathbb{Q}\left(\sqrt{-11}\right), \mathbb{Q}\left(\sqrt{-19}\right),$$
$$\mathbb{Q}\left(\sqrt{-43}\right), \mathbb{Q}\left(\sqrt{-67}\right), \mathbb{Q}\left(\sqrt{-163}\right)$$

השערה. יש אינסוף שדות ריבועיים ממשיים עם $h_K = 1$.

2.6 משפט היחידות של דיריכלה

ראינו סדרת העתקות

$$1 \to \mathcal{O}_K^\times \to K^\times \xrightarrow[\alpha \mapsto \alpha\mathcal{O}_K]{} \mathcal{P}_K \to \mathcal{J}_K \to \mathrm{Cl}_K \to 0.$$

נרצה להבין את $\mathcal{O}_K^\times$. נוכיח את המשפט הבא:

משפט 2.27 (משפט היחידות של דיריכלה). **יהי K שדה מספרים, יהי r מספר השיכונים הממשיים $K \hookrightarrow \mathbb{R}$, ויהי s מספר הזוגות של שיכונים צמודים $K \hookrightarrow \mathbb{C}$ (בפרט, מתקיים $n = [K:\mathbb{Q}] = r + 2s$). אזי**

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1},$$

כאשר $\mu(K)$ הינה חבורת כל שורשי היחידה ב-$\mathcal{O}_K^\times$.

הוכחה. נגדיר $V = \mathbb{R}^r \times \mathbb{C}^s$, שהוא מרחב וקטורי ממימד n מעל $\mathbb{R}$. אם $\sigma_1, \ldots, \sigma_r : K \hookrightarrow \mathbb{R}$ השיכונים הממשיים ו-$\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s} : K \hookrightarrow \mathbb{C}$ השיכונים המרוכבים, אפשר להגדיר $\theta : K \hookrightarrow V$ לפי

$$\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \tau_1(\alpha), \ldots, \tau_s(\alpha)).$$

על V יש טופולוגיה (טופולוגיית המכפלה הנובעת מהטופולוגיות הסטנדרטיות של $\mathbb{R}$ ושל $\mathbb{C}$). בנוסף, אפשר להגדיר על V נורמה רציפה $N : V \to \mathbb{R}$ לפי

$$N(x_1, \ldots, x_r, z_1, \ldots, z_s) = x_1 \ldots x_r |z_1|^2 \ldots |z_s|^2.$$

נשים לב כי

$$\mathrm{N}(\theta(\alpha)) = \sigma_1(\alpha) \ldots \sigma_r(\alpha) \tau_1(\alpha) \overline{\tau_1}(\alpha) \ldots \tau_s(\alpha) \overline{\tau_s}(\alpha) = \mathrm{N}_{K/\mathbb{Q}}(\alpha).$$

עוד נשים לב כי $\mathcal{O}_K^\times = \left\{\alpha \in K : \left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right| = 1\right\}$. נסמן $V^\times = (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s$, ונגדיר

$$G = \{v \in V : |\mathrm{N}(v)| = 1\} \subseteq V^\times.$$

G קבוצה סגורה ב-V, כי $G = \mathrm{N}^{-1}(\{-1,1\})$, ולכן G סגורה גם ב-$V^\times$. נגדיר $U = \theta(\mathcal{O}_K^\times) = G \cap \theta(\mathcal{O}_K)$. כיוון ש-$\theta$ חח"ע, $\theta(\mathcal{O}_K^\times) \cong \mathcal{O}_K^\times$, ולכן שקול להבין את $\theta(\mathcal{O}_K^\times)$. נציין בנוסף כי G חבורה כפלית.

נטען כי $\theta(\mathcal{O}_K) \subseteq V$ שריג. אכן, $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$, לכן $\theta(\mathcal{O}_K) = \mathbb{Z} \cdot \theta(\alpha_1) + \cdots + \mathbb{Z} \cdot \theta(\alpha_n)$, וה-$\theta(\alpha_i)$-ים בלתי-תלויים לינארית בגלל אי-התלות של האוטומורפיזמים $\sigma_1, \ldots, \sigma_r, \tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$.

למה. המנה G/U היא קומפקטית.

הוכחה. נשים לב שלכל $v \in V^\times$, הכפל ב-v הינה העתקה $\mathbb{R}$-לינארית $V \to V$ המיוצגת על ידי מטריצה עם דטרמיננטה $\mathrm{N}(v)$. זה אומר שאם $X \subseteq V$ קבוצה בעלת נפח סופי, אזי

$$\mathrm{vol}(vX) = |\mathrm{N}(v)| \cdot \mathrm{vol}(X)$$

כאשר $vX = \{vx : x \in X\}$.

תהי X קבוצה סימטרית, קמורה וקומפקטית כך ש-$\mathrm{vol}(X) > 2^n \cdot \mathrm{vol}(\theta(\mathcal{O}_K))$. X קומפקטית, לכן $\mathrm{N}(X) = \{\mathrm{N}(x) : x \in X\} \subseteq \mathbb{R}$ קומפקטית, ובפרט קיים M כך ש-$|\mathrm{N}(x)| \le M$ לכל $x \in X$. נזכור כי יש רק מספר סופי של אידאלים ב-$\mathcal{O}_K$ (ובפרט אידאלים ראשוניים) מנורמה $\ge M$. נסמן את האידאלים הראשיים הללו על ידי $a_1\mathcal{O}_K, \ldots, a_m\mathcal{O}_K$.

יהי $g \in G$ כלשהו. אזי $\mathrm{vol}\left(g^{-1}X\right) = \mathrm{vol}(X)$, ולפי מינקובסקי (טענה 2.22) קיים $0 \neq \alpha \in \mathcal{O}_K$ כך ש-$\theta(\alpha) \in g^{-1}X$. בפרט מתקיים $|\mathrm{N}(\theta(\alpha))| = \left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right| \le M$, כלומר $\mathrm{N}(\alpha\mathcal{O}_K) \le M$. לכן $\alpha = a_i u$ עבור i מתאים ו-$u \in \mathcal{O}_K^\times$.

הראינו שלכל $g \in G$ קיים i שעבורו $g^{-1}X \cap \theta(a_i)U \neq \varnothing$, ובאופן שקול

$$\theta\left(a_i^{-1}\right)X \cap gU \neq \varnothing.$$

בפרט, בקבוצה $Y = \underbrace{\bigcup_{i=1}^{m} \theta\left(a_i^{-1}\right)X}_{\text{compact}} \cap \underbrace{G}_{\text{closed}}$ יש נציג של כל מחלקה של G/U. אך Y קומפקטית, ההטלה $\varphi : G \to G/U$ רציפה ו-$\varphi(Y) = G/U$, ולכן G/U קבוצה קומפקטית. □

נסתכל על ההעתקה הלוגריתמית $L : V^\times \to \mathbb{R}^{r+s}$ הנתונה על ידי

$$(x_1, \ldots, x_r, z_1, \ldots, z_s) \mapsto (\log|x_1|, \ldots, \log|x_r|, 2\log|z_1|, \ldots, 2\log|z_s|)$$

(שהיא הומומורפיזם של חבורות). נגדיר משטח-על

$$H = \left\{(y_1, \ldots, y_{r+s}) \in \mathbb{R}^{r+s} : y_1 + \cdots + y_{r+s} = 0\right\}$$

ברור כי $H \cong \mathbb{R}^{r+s-1}$; נשים לב כי $L(G) = H$.

למה. $(\ker L) \cap U = \theta(\mu(K))$.

הוכחה. ראשית, $\ker L = \{\pm 1\}^r \times \left(S^1\right)^s$ קומפקטית ב-$V^\times$. U סגורה ואפילו דיסקרטית ב-$V^\times$; לכן $(\ker L) \cap U$ קומפקטית ודיסקרטית, ומכאן ש-$(\ker L) \cap U$ הינה חבורה סופית. כל איבר שלה הינו $\theta(\alpha)$ עבור $\alpha \in K^\times$. אם נסמן $N = |(\ker L) \cap U|$, אזי

$$\theta\left(\alpha^N\right) = (1, \ldots, 1) \Longrightarrow \alpha^N = 1.$$

הראינו את ההכלה $\subseteq$. אך ההכלה השנייה ברורה, ולכן נקבל את השוויון הדרוש. □

למה. $L(U)$ תת-חבורה דיסקרטית של $H = L(G)$, כלומר שריג.

הוכחה. מספיק להוכיח שכל קופסה סגורה $B = \{(y_1, \ldots, y_{r+s}) \in \mathbb{R}^{r+s} : |y_i| \le \varepsilon\}$ מכילה מספר סופי של איברים מ-$L(U)$.

יהי $\alpha \in \mathcal{O}_K^\times$ כך ש-$L(\theta(\alpha)) \in B$. אזי $|\sigma_i(\alpha)| \le e^\varepsilon$, ו-$|\tau_i(\alpha)| \le e^{\varepsilon/2}$. נתבונן בפולינום

$$\prod_{i=1}^{r}(T - \sigma_i(\alpha)) \cdot \prod_{j=1}^{s}(T - \tau_j(\alpha))\left(T - \overline{\tau_j}(\alpha)\right).$$

לפי תורת גלואה, זהו פולינום עם מקדמים שלמים. לפי החסמים הנ"ל, נקבל חסמים על הערכים המוחלטים של מקדמי הפולינום. אך יש מספר סופי של פולינומים עם מקדמים חסומים כך, ולכל אחד מהם מספר סופי של שורשים – ולכן יש מספר אפשרויות סופי עבור α, כנדרש. □

למה. $L\left(U\right)$ הינו שריג שלם ב-H.

הוכחה. $L:G\to L\left(G\right)$ רציפה ועל, ולכן משרה העתקה רציפה ועל $G/U\to L(G)/L(U)$. מכאן שגם $L(G)/L(U)$ קומפקטית. לכן אפשר למצוא תחום יסודי חסום B כך שמתקיים $H=L\left(G\right)=\bigcup_{\gamma\in L(U)}\left(B+\gamma\right)$. לפי טענה 2.19, $L\left(U\right)$ שריג שלם ב-H. $\square$

אם כן, קיבלנו סדרה מדויקת של חבורות

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (\ker L)\cap U & \longrightarrow & U & \longrightarrow & L\left(U\right) & \longrightarrow & 1 \\ & & \wr\| & & & & \wr\| & & \\ & & \mu\left(K\right) & & & & \mathbb{Z}^{r+s-1} & & \end{array}$$

ואנחנו רוצים להוכיח כי $U\cong\mu\left(K\right)\times\mathbb{Z}^{r+s-1}$. זה ינבע מלמה מתורת החבורות:

למה. תהי

$$1\to A\xrightarrow{i}B\xrightarrow{\varphi}\mathbb{Z}^m\to 1$$

סדרה מדויקת של חבורות אבליות. אזי $B\cong A\times\mathbb{Z}^m$.

הוכחה. יהי $e_1,\ldots,e_m$ בסיס של $\mathbb{Z}^m$. נבחר $b_1,\ldots,b_m\in B$ כך ש-$\varphi\left(b_i\right)=e_i$, ונגדיר $\psi:A\times\mathbb{Z}^m\to B$ לפי

$$\psi\left(a,\sum_{j=1}^{m}n_je_j\right)=i\left(a\right)+\sum_{j=1}^{m}n_jb_j.$$

ψ מגדירה הומומורפיזם של חבורות.

נראה ש-ψ חח"ע: נניח

$$\psi\left(a,\sum_{j=1}^{m}n_je_j\right)=i\left(a\right)+\sum_{j=1}^{m}n_jb_j=0.$$

נפעיל φ על השוויון, ונקבל

$$\sum_{j=1}^{m}n_je_j=0.$$

כיוון ש-$e_1,\ldots,e_m$ בסיס של $\mathbb{Z}^m$, $n_1=\cdots=n_m=0$. לכן $i\left(a\right)=0$, וכיוון ש-i חח"ע נקבל $a=0$.

כעת נראה ש-ψ על: יהי $b\in B$. נרשום $\varphi\left(b\right)=\sum_{j=1}^{m}n_je_j$. אזי

$$\varphi\left(b-\sum_{j=1}^{m}n_jb_j\right)=0$$

ולכן $b-\sum_{j=1}^{m}n_jb_j\in\ker\varphi=\operatorname{Im}i$, כלומר $b-\sum_{j=1}^{m}n_jb_j=i\left(a\right)$ לאיזשהו $a\in A$. במילים אחרות,

$$\psi\left(a,\varphi\left(b\right)\right)=b.$$

בסך הכל, ψ איזומורפיזם, כלומר $B\cong A\times\mathbb{Z}^m$. $\square$

$\square$

הגדרה 2.28. נניח כי השדה K מקיים $r+s-1=1$ (כלומר $\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}$). איבר הפיך היוצר את $\mathcal{O}_K^\times$ (מודולו $\mu(K)$) נקרא ***יחידה יסודית*** (**fundamental unit**).

דוגמה 2.29. נמצא את פתרונות המשוואה $x^2-7y^2=1$ מעל $\mathbb{Z}$.
נשים לב ש-(x,y) פתרון של המשוואה אם ורק אם $\mathrm{N}_{\mathbb{Q}(\sqrt{7})/\mathbb{Q}}\left(x+y\sqrt{7}\right)=1$, ובפרט $x+y\sqrt{7}$ הפיך ב-$\mathbb{Z}\left[\sqrt{7}\right]$. אין איברים הפיכים מנורמה -1, כי -1 אינו נורמה מודולו 7; לכן אנחנו רוצים למצוא את כל האיברים ההפיכים. מתקיים

$$\mathcal{O}_{\mathbb{Q}(\sqrt{7})}=\mathbb{Z}\left[\sqrt{7}\right] \Longrightarrow \mathcal{O}_{\mathbb{Q}(\sqrt{7})}^\times \cong \mu\left(\mathbb{Q}\left(\sqrt{7}\right)\right) \times \mathbb{Z}^{r+s-1}.$$

אצלנו $\mu\left(\mathbb{Q}\left(\sqrt{7}\right)\right) \cong \{\pm 1\}$, $r=2$ ו-$s=0$, לכן

$$\mathcal{O}_{\mathbb{Q}(\sqrt{7})}^\times \cong \{\pm 1\} \times \mathbb{Z}.$$

אם נבחר יוצר ε של $\mathbb{Z}$, כלומר יחידה יסודית, אזי

$$\mathcal{O}_{\mathbb{Q}(\sqrt{7})}^\times = \{\pm\varepsilon^n : n \in \mathbb{Z}\}.$$

במקרה הזה, ניתן לבדוק כי $8+3\sqrt{7}$ יחידה יסודית.

3 אידאלים ראשוניים בתחומי דדקינד

מוטיבציה. ניקח $K=\mathbb{Q}\left(\sqrt{7}\right)$. מהו h_K? במקרה הזה, $n=2$, $r=2$ ו-$s=0$, ולכן חסם מינקובסקי נותן

$$\mathrm{N}(I) \le \left(\frac{4}{\pi}\right)^0 \cdot \frac{2}{4} \cdot \sqrt{28} = \sqrt{7} < 3.$$

כלומר, בכל מחלקה יש אידאל מנורמה 1 ($\mathcal{O}_K$=) או 2. אם $\mathrm{N}(I)=2$, אזי I ראשוני וכן מקיים $I \mid 2\mathcal{O}_K$.
לכן נרצה לחקור את הפירוק $2\mathcal{O}_K = P_1 \ldots P_r$. $\mathrm{N}(2\mathcal{O}_K)=4$, כלומר יש שתי אפשרויות: או שהוא נשאר ראשוני, או שהוא מתפרק למכפלה של שני ראשוניים.

שאלה. יהי K שדה מספרים, ויהי p מספר ראשוני. מהו הפירוק של $p\mathcal{O}_K$ כמכפלה של אידאלים ראשוניים $p\mathcal{O}_K = P_1^{e_1} \ldots P_r^{e_r}$, כאשר $P_1,\ldots,P_r \subseteq \mathcal{O}_K$ שונים זה מזה?

3.1 הסתעפות של ראשוניים בשדות מספרים

הגדרה 3.1. p נקרא **מסועף** (**ramified**) ב-K אם $e_i > 1$ לאיזשהו i.

טענה 3.2. יהי K שדה מספרים. אזי p מסועף ב-K אם ורק אם $p \mid \mathrm{d}_K$. בפרט, יש מספר סופי של ראשוניים מסועפים ב-K.

הוכחה. יהי A תחום שלמות, ותהי $A\subseteq B$ הרחבה של חוגים כך ש-B הינו A-מודול חופשי נוצר סופית. יהי $x_1,\dots,x_n$ בסיס של B מעל A. לכל $b\in B$ נתבונן בהעתקה ה-A-לינארית $m_b:B\to B$ הנתונה על ידי $m_b(x)=bx$. תהי $\mathrm{Tr}_{B/A}(b)\in A$ העקבה של המטריצה של m_b ביחס לבסיס $x_1,\dots,x_n$, ונגדיר

$$\mathrm{disc}_{B/A}(x_1,\dots,x_n)=\det\left(\mathrm{Tr}_{B/A}(x_ix_j)\right)\in A$$

כפי שראינו, אם ניקח בסיס אחר נקבל

$$\mathrm{disc}_{B/A}(y_1,\dots,y_n)=\mathrm{disc}_{B/A}(x_1,\dots,x_n)\cdot(\det M)^2$$

כאשר M מטריצת המעבר בין הבסיסים. מעתה נרשום $\mathrm{disc}_{B/A}$, בהבנה שזה מוגדר עד כדי כפל באיבר של $(A^*)^2$; עם זאת, התנאי $\mathrm{disc}_{B/A}=0$ מוגדר היטב.

טענה. יהיו B_1 ו-B_2 הרחבות כנ"ל של A. אזי $\mathrm{disc}_{B_1\times B_2/A}=\mathrm{disc}_{B_1/A}\cdot\mathrm{disc}_{B_2/A}$.

הוכחה. יהי $x_1,\dots,x_n$ בסיס של B_1, ויהי $y_1,\dots,y_m$ בסיס של B_2. אז אפשר לקבל בסיס של $B_1\times B_2$ על ידי $(x_1,0),\dots,(x_n,0),(0,y_1)\dots,(0,y_m)$. נבין את $\mathrm{disc}_{B_1\times B_2/A}$:

- כיוון ש-$(x_i,0)\cdot(0,y_j)=0$, $\mathrm{Tr}_{B_1\times B_2/A}((x_i,0)\cdot(0,y_j))=0$.
- המטריצה של $m_{(x_i,0)\cdot(x_j,0)}=m_{(x_ix_j,0)}$ הינה

$$\left(\begin{array}{c|c} m_{x_ix_j}\text{ over }B_1 & 0\\ \hline 0 & 0\end{array}\right)$$

ולכן $\mathrm{Tr}_{B_1\times B_2/A}((x_i,0)\cdot(x_j,0))=\mathrm{Tr}_{B_1/A}(x_ix_j)$.

- בדומה, $\mathrm{Tr}_{B_1\times B_2/A}((0,y_i)\cdot(0,y_j))=\mathrm{Tr}_{B_2/A}(y_iy_j)$.

לכן, $\mathrm{disc}_{B_1\times B_2/A}$ הינה הדטרמיננטה של

$$\left(\begin{array}{c|c} \mathrm{Tr}_{B_1/A}(x_ix_j) & 0\\ \hline 0 & \mathrm{Tr}_{B_2/A}(y_iy_j)\end{array}\right)$$

והכפליות נובעת. □

טענה. יהי K שדה מספרים, ויהי p מספר ראשוני. באופן טבעי $\mathcal{O}_K/p\mathcal{O}_K$ הינו מודול של $\mathbb{F}_p$. אזי

$$\mathrm{disc}_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{F}_p}\equiv \mathrm{d}_K\pmod p.$$

(ליתר דיוק, אגף ימין נמצא ב-$\mathbb{F}_p$, ואילו אגף שמאל מוגדר ב-$\mathbb{F}_p/(\mathbb{F}_p^*)^2$, ולכן אגף ימין צריך להיות שייך לאגף שמאל.)

הוכחה. יהי $\alpha_1,\dots,\alpha_n$ בסיס שלם של K, $\mathcal{O}_K=\mathbb{Z}\alpha_1+\dots+\mathbb{Z}\alpha_n$. לכן

$$\mathcal{O}_K/p\mathcal{O}_K=\mathbb{F}_p\overline{\alpha_1}+\dots+\mathbb{F}_p\overline{\alpha_n}$$

כאשר $\overline{\alpha_i}\in\mathcal{O}_K/p\mathcal{O}_K$ הרדוקציה של α_i. לכן

$$\mathrm{Tr}_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{F}_p}(\overline{\alpha_i}\cdot\overline{\alpha_j})\equiv\mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}}(\alpha_i\alpha_j)\pmod p.$$

נשים לב שהרדוקציות $\overline{\alpha_1},\dots,\overline{\alpha_n}$ הן בסיס, כי $\mathrm{N}_{K/\mathbb{Q}}(p)=p^n=\mathrm{N}(p\mathcal{O}_K)$. כשנעבור לדטרמיננטות יישמר השוויון הנ"ל, וזה מוכיח את תת-הטענה. □

נחזור לטענה. לפי תת-הטענה השנייה, $p \mid \mathrm{d}_K$ אם ורק אם $\mathrm{disc}_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{F}_p} = 0$. נשים לב שאם $p\mathcal{O}_K = P_1^{e_1} \dots P_r^{e_r}$, ממשפט השאריות הסיני נקבל

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/P_1^{e_1} \times \dots \times \mathcal{O}_K/P_r^{e_r}.$$

לפי תת-הטענה הראשונה,

$$\mathrm{disc}_{(\mathcal{O}_K/p\mathcal{O}_K)/\mathbb{F}_p} = \prod_{i=1}^{r} \mathrm{disc}_{\left(\mathcal{O}_K/P_i^{e_i}\right)/\mathbb{F}_p},$$

ולכן $p \mid \mathrm{d}_K$ אם ורק אם $\mathrm{disc}_{\left(\mathcal{O}_K/P_i^{e_i}\right)/\mathbb{F}_p} = 0$ לאיזשהו i.

אם כן, מספיק להוכיח ש-$\mathrm{disc}_{(\mathcal{O}_K/P^e)/\mathbb{F}_p} = 0$ אם ורק אם $e > 1$.

- אם $e = 1$, $\mathcal{O}_K/P$ הינו שדה. לכן $\mathbb{F}_p \subseteq \mathcal{O}_K/P$ הרחבה ספרבילית של שדות, ולפי טענה 1.23 נקבל $\mathrm{disc}_{(\mathcal{O}_K/P)/\mathbb{F}_p} \neq 0$.
- נניח $e > 1$, ויהי $x \in P \setminus P^e$. כיוון ש$\mathbb{F}_p$ שדה, ניתן להשלים את x ל-$\mathbb{F}_p$-בסיס של $\mathcal{O}_K/P^e$, נסמנו $x_1 = x, \dots, x_m$. לכל $y \in \mathcal{O}_K/P^e$ מתקיים $(x_1 x_j)^e y = 0$, כי $x_1^e = 0$. זה אומר ש-$m_{x_1 x_j}^e = 0$. לכן כל הערכים העצמיים של $m_{x_1 x_j}$ הם 0, ומכאן $\mathrm{Tr}_{(\mathcal{O}_K/P^e)/\mathbb{F}_p}(x_1 x_j) = 0$. מכאן שהשורה הראשונה של המטריצה $\left(\mathrm{Tr}_{(\mathcal{O}_K/P^e)/\mathbb{F}_p}(x_i x_j)\right)$ כולה אפסים, ולכן $\mathrm{disc}_{(\mathcal{O}_K/P^e)/\mathbb{F}_p} = 0$.

□

3.2 פירוק של אידאלים ראשוניים בהרחבות של תחומי דדקינד

נחזור לסיטואציה של תחומי דדקינד. כלומר: A הוא תחום דדקינד, K שדה השברים שלו, L/K הרחבה סופית וספרבילית ו-B הסגור השלם של A ב-L. בפרט, B תחום דדקינד.

טענה 3.3. יהי $\mathfrak{p} \subseteq A$ אידאל ראשוני. אזי $\mathfrak{p}B \neq B$.

הוכחה. אם $\mathfrak{p} = 0$, הטענה ברורה; לכן נניח $\mathfrak{p} \neq 0$. ניקח $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ (מיחידות הפירוק לאידאלים ראשוניים, $\mathfrak{p}^2 \neq \mathfrak{p}$, כלומר $\mathfrak{p}^2 \subsetneq \mathfrak{p}$, ולכן אפשר למצוא π כזה). לכן $\pi A = \mathfrak{p} \cdot I$ כאשר $\mathfrak{p}$ ו-I זרים, כלומר $A = I + \mathfrak{p}$. נכתוב $1 = b + c$ כאשר $b \in \mathfrak{p}$ ו-$c \in I$.

נניח בשלילה כי $\mathfrak{p}B = B$. אזי $cB = c\mathfrak{p}B \subseteq I\mathfrak{p}B = \pi AB = \pi B$, כלומר $c = \pi x$ לאיזשהו $x \in B$. מצד שני, $x = \frac{c}{\pi} \in \mathrm{Frac}A = K$, ומכאן $x \in B \cap K$. לכן $x \in K$ שלם מעל A, ו-A סגור בשלמות, ומכאן $x \in A$. אבל אז $c \in \pi A \subseteq \mathfrak{p}$, ובפרט $1 = b + c \in \mathfrak{p}$, בסתירה. □

הגדרה 3.4. יהי $\theta \in L$ איבר פרימיטיבי (כלומר $L = K(\theta)$). בלי הגבלת הכלליות, נניח $\theta \in B$. **המוליך (conductor)** של θ הינו

$$\mathcal{F}_\theta = \{x \in B : xB \subseteq A[\theta]\}.$$

במילים, $\mathcal{F}_\theta$ הינו האידאל הכי גדול של B שמוכל ב-$A[\theta]$. לרוב נשמיט את θ, כי הוא יהיה ברור מההקשר.

בפרט, $\mathcal{F}_\theta = B$ אם ורק אם $B = A[\theta]$.

משפט 3.5. יהי $\theta\in B$ כנ"ל, יהי $0\neq\mathfrak{p}\subseteq A$ אידאל ראשוני כך ש-$\mathfrak{p}B$ ו-$\mathcal{F}_\theta$ זרים, ויהי $g(x)\in A[x]$ הפולינום המינימלי (המתוקן) של θ. יהי $k={}^{A}/_{\mathfrak{p}}$ שדה השאריות, ויהי

$$\overline{g}(x)=\overline{g_1}(x)^{e_1}\dots\overline{g_r}(x)^{e_r}$$

הפירוק של הרדוקציה $\overline{g}(x)\in k[x]$ לגורמים אי-פריקים (שונים). אזי:

א. $\mathfrak{p}B=P_1^{e_1}\dots P_r^{e_r}$, כאשר $P_i=\mathfrak{p}B+g_i(\theta)B$ עבור $g_i(x)\in A[x]$ שהוא הרמה של $\overline{g_i}(x)$.

ב. לכל $1\leq i\leq r$, יהי $f_i=[{}^{B}/_{P_i}:k]$. אזי $f_i=\deg\overline{g_i}(x)$.

ג. (הנוסחה היסודית) יהי $n=[L:K]$. אזי $n=\sum_{i=1}^{r}e_if_i$.

הוכחה.

א. יהי $B'=A[\theta]$.

טענה. ההעתקה $\varphi:B'\hookrightarrow B\twoheadrightarrow {}^{B}/_{\mathfrak{p}B}$ הינה על.

הוכחה. לפי ההנחה, $\mathfrak{p}B+\mathcal{F}_\theta=B$. זה אומר שכל מחלקה של ${}^{B}/_{\mathfrak{p}B}$ מכילה איבר של $\mathcal{F}_\theta\subseteq B'$. לכן ההעתקה הינה על. $\square$

טענה. ההכלה $B'\subseteq B$ משרה איזומורפיזם ${}^{B'}/_{\mathfrak{p}B'}\to {}^{B}/_{\mathfrak{p}B}$.

הוכחה. מספיק להוכיח כי $\mathfrak{p}B'$ הינו הגרעין של φ. ברור כי $\mathfrak{p}B'\subseteq\ker\varphi$ וכי $\ker\varphi=B'\cap\mathfrak{p}B$. נשים לב כי

$$B'\cap\mathfrak{p}B\subseteq B(B'\cap\mathfrak{p}B)=(\mathfrak{p}B+\mathcal{F}_\theta)(B'\cap\mathfrak{p}B).$$

מהגדרת $\mathcal{F}_\theta$, $\mathcal{F}_\theta B\subseteq B'$, ובפרט $\mathcal{F}_\theta(B'\cap\mathfrak{p}B)\subseteq\mathcal{F}_\theta(\mathfrak{p}B)\subseteq\mathfrak{p}B'$. בנוסף,

$$\mathfrak{p}B(B'\cap\mathfrak{p}B)\subseteq(\mathfrak{p}B)(\mathfrak{p}B)=\mathfrak{p}^2B.$$

קיבלנו

$$B'\cap\mathfrak{p}B\subseteq\mathfrak{p}B'+\mathfrak{p}^2B\subseteq\left(\mathcal{F}_\theta+\mathfrak{p}^2B\right)\left(\mathfrak{p}B'+\mathfrak{p}^2B\right)\subseteq\mathcal{F}_\theta\mathfrak{p}B'+\mathfrak{p}^3B=\mathfrak{p}B'+\mathfrak{p}^3B$$

וכך ניתן להמשיך. בסך הכל

$$B'\cap\mathfrak{p}B\subseteq\bigcap_{n=1}^{\infty}(\mathfrak{p}B'+\mathfrak{p}^nB)\underset{\bigcap_{n=1}^{\infty}\mathfrak{p}^n=0}{=}\mathfrak{p}B'$$

כנדרש. $\square$

מתקיים $B'=A[\theta]\cong {}^{A[x]}/_{g(x)}$; לכן,

$${}^{B'}/_{\mathfrak{p}B'}={}^{A[x]}/_{(\mathfrak{p},g(x))}\cong {}^{k[x]}/_{\overline{g}(x)}\cong {}^{k[x]}/_{\overline{g_1}(x)^{e_1}}\times\cdots\times {}^{k[x]}/_{\overline{g_r}(x)^{e_r}}.$$

הגורמים הראשוניים של $\mathfrak{p}B$ הם הראשוניים ב-B שמכילים את $\mathfrak{p}B$, ואלה מתאימים לאידאלים הראשוניים של ${}^{B}/_{\mathfrak{p}B}\cong {}^{k[x]}/_{g(x)}$. האידאלים הראשוניים של ${}^{k[x]}/_{g(x)}$ הם

$\overline{P_i} = (\overline{g_i}(x))$. ב-$B$ הם מתאמים לאידאלים $P_i = g_i(\theta)B + \mathfrak{p}B$ כאשר g_i הרמה כלשהי של $\overline{g_i}$.

נשים לב כי $P_1^{e_1} \ldots P_r^{e_r} \subseteq \mathfrak{p}B$; אכן, המכפלה נוצרת על ידי איברים מהצורה

$$\prod_{i=1}^{r}\prod_{j=1}^{e_i}\left(g_i(\theta)x_{i,j} + y_{i,j}\right) \in \underbrace{\prod_{i=1}^{n} g_i(\theta)^{e_i}}_{\in \mathfrak{p}B} \cdot x + \mathfrak{p}B \subseteq \mathfrak{p}B$$

עבור $x_{i,j} \in B$ ו-$y_{i,j} \in \mathfrak{p}B$.

מצד שני, הפירוק של $\mathfrak{p}B$ לראשוניים הוא $\mathfrak{p}B = P_1^{a_1} \ldots P_r^{a_r}$. הוכחנו $\mathfrak{p}B \mid P_1^{e_1} \ldots P_r^{e_r}$, כלומר $a_i \le e_i$. נניח בשלילה כי $a_i < e_i$ לאיזשהו i. התמונה של $P_1^{a_1} \ldots P_r^{a_r}$ במנה $B/\mathfrak{p}B \cong k[x]/\overline{g}(x)$ הינה $\prod_{i=1}^{r} \overline{g_i}(x)^{a_i} \ne 0$ (כי המעלה שלו קטנה יותר משל $\overline{g}(x)$); אבל זו סתירה, כי המנה של $\mathfrak{p}B$ היא 0.

ב. מתקיים $B/P_i \cong k[x]/\overline{g_i}(x)$. לכן

$$f_i = [B/P_i : k] = [k[x]/\overline{g_i}(x) : k] = \deg \overline{g_i}(x).$$

ג. $\deg g(x) = [L:K] = n$, כי $g(x)$ הוא הפולינום המינימלי של θ. אבל $g(x)$ מתוקן, לכן

$$n = \deg g(x) = \sum_{i=1}^{r} e_i \deg \overline{g_i}(x) = \sum_{i=1}^{r} e_i f_i.$$

□

דוגמה 3.6. ניקח $L = \mathbb{Q}\left(\sqrt{-1}\right)$. לפי תרגיל 1.8, $\mathcal{O}_L = \mathbb{Z}\left[\sqrt{-1}\right]$. יהי p מספר ראשוני. נרצה ללמוד את הפירוק של $p\mathcal{O}_L$ לאידאלים ראשוניים. ניקח $\theta = \sqrt{-1}$. מתקיים $\mathcal{O}_L = \mathbb{Z}[\theta]$, ולכן $\mathcal{F}_\theta = \mathcal{O}_L$. מכאן שלכל $p \in \mathbb{Z}$ ראשוני אפשר להשתמש במשפט 3.5 עבור $\mathfrak{p} = p\mathbb{Z}$. הפולינום המינימלי של θ הוא $g(x) = x^2 + 1$. נחלק לשני מקרים:

- $\boxed{p=2}$ מתקיים $\overline{g}(x) = x^2 + 1 \equiv (x+1)^2 \pmod 2$, לכן $2\mathcal{O}_L = P^2$. נשים לב כי $2 = \left(1+\sqrt{-1}\right)\left(1-\sqrt{-1}\right)$, לכן

$$P = \left(2, 1+\sqrt{-1}\right) = \left(1+\sqrt{-1}\right).$$

זה מראה ש-2 מסועף ב-$\mathbb{Q}\left(\sqrt{-1}\right)$, ואכן $d_L = -4$.

- $\boxed{p>2}$ הפולינום x^2+1 מתפרק מודולו p אם ורק אם יש לו שורש מודולו p. החבורה $\mathbb{F}_p^\times$ ציקלית מסדר $p-1$, לכן $y \in \mathbb{F}_p^\times$ שורש של x^2+1 אם ורק אם $o(y) = 4$, אם ורק אם $4 \mid p-1$, אם ורק אם $p \equiv 1 \pmod 4$.
לכן, אם $p \equiv 1 \pmod 4$ מתקיים $x^2+1 \equiv (x+a)(x-a) \pmod p$ עבור איזשהו $a \in \mathbb{Z}$; אז $p\mathcal{O}_L = P_1 \cdot P_2$, כאשר $P_1 = \left(p, a+\sqrt{-1}\right)$ ו-$P_2 = \left(p, a-\sqrt{-1}\right)$.
לעומת זאת, אם $p \equiv 3 \pmod 4$, הפולינום x^2+1 אי-פריק מודולו p, ולכן האידאל $p\mathcal{O}_L$ נשאר ראשוני.

כמסקנה, נוכל להוכיח תוצאה בסיסית מתורת המספרים:

משפט (משפט לגראנז'). יהי p ראשוני. אזי p הוא סכום של שני ריבועים אם ורק אם $p=2$ או $p\equiv 1 \pmod 4$.

הוכחה. נשתמש בסימונים מהדוגמה. עבור $a,b\in\mathbb{Z}$,

$$\mathrm{N}_{L/\mathbb{Q}}\left(a+b\sqrt{-1}\right)=\left(a+b\sqrt{-1}\right)\left(a-b\sqrt{-1}\right)=a^2+b^2.$$

כלומר, p הוא סכום של שני ריבועים אם ורק אם ב-$\mathcal{O}_L$ קיים איבר α_p מנורמה p. אבל אז האידאל $\alpha_p\mathcal{O}_L$ מקיים $\mathrm{N}\left(\alpha_p\mathcal{O}_L\right)=\mathrm{N}_{L/\mathbb{Q}}\left(\alpha_p\right)=p$, ובפרט $\alpha_p\mathcal{O}_L$ ראשוני. בנוסף, $\alpha_p\mathcal{O}_L$ מחלק את $p\mathcal{O}_L$. נחלק למקרים:

- $\boxed{p=2}$ יש אידאל ראשוני יחיד P המחלק את $2\mathcal{O}_L$, וראינו ש-$2\mathcal{O}_L=P^2$. לכן

  $$\mathrm{N}\left(2\mathcal{O}_L\right)=\mathrm{N}_{L/\mathbb{Q}}(2)=4\Longrightarrow \mathrm{N}(P)=2.$$

  ראינו באמצעות חסם מינקובסקי (טענה 2.26) כי $\mathcal{O}_L$ תחום ראשי, ולכן יוצר של P יהיה איבר מנורמה 2 כנדרש.

- $\boxed{p\equiv 1 \pmod 4}$ במקרה זה $p\mathcal{O}_L=P_1\cdot P_2$, לכן $\mathrm{N}\left(P_1\right)\cdot\mathrm{N}\left(P_2\right)=p^2$, ומכאן $\mathrm{N}\left(P_1\right)=\mathrm{N}\left(P_2\right)=p$. אבל P_1,P_2 ראשיים, לכן היוצרים הם איברים מנורמה p.

- $\boxed{p\equiv 3 \pmod 4}$ אז $p\mathcal{O}_L$ ראשוני מנורמה p^2, ולכן אין איבר ב-$\mathcal{O}_L$ מנורמה p.

$\square$

בשתי הדוגמאות הבאות נכליל את דוגמה 3.6 עבור $L=\mathbb{Q}\left(\sqrt{d}\right)$.

דוגמה 3.7. יהי $d\equiv 2,3 \pmod 4$ חופשי מריבועים. במקרה הזה, $\mathcal{O}_L=\mathbb{Z}\left[\sqrt{d}\right]$, ואפשר לקחת $\theta=\sqrt{d}$. מתקיים $\mathcal{F}_\theta=\mathcal{O}_L$. הדיסקרימיננטה היא $d_L=4d$, ולכן p מסתעף אם ורק אם $p=2$ או $p\mid d$. אחרת,

- $p\mathcal{O}_L=P_1\cdot P_2$ אם ורק אם $g(x)=x^2-d$ מתפרק מודולו p, אם ורק אם יש פתרון למשוואה $x^2\equiv d \pmod p$.
- $p\mathcal{O}_L$ ראשוני אם ורק אם אין פתרון למשוואה $x^2\equiv d \pmod p$.

דוגמה 3.8. כעת נניח $d\equiv 1 \pmod 4$. אז $\mathbb{Z}\left[\sqrt{d}\right]\subsetneq\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]=\mathcal{O}_L$. יש שתי אפשרויות "טבעיות" לבחירת θ:

- $\theta=\frac{1+\sqrt{d}}{2}$; אז $\mathcal{F}_\theta=\mathcal{O}_L$, אבל $g(x)=x^2-x+\frac{1-d}{4}$ לא "נחמד" במיוחד.
- $\theta=\sqrt{d}$; אז $g(x)=x^2-d$, אבל $\mathcal{F}_\theta\neq\mathcal{O}_L$, ועשויה להיות בעיה בתנאי המשפט.

נלך על האופציה השנייה, ונבדוק לאילו ראשוניים p מתקיים ש-$p\mathcal{O}_L$ אינו זר ל-$\mathcal{F}_\theta$. אם הם לא זרים, זה אומר ש-$\mathcal{F}_\theta\subseteq P$ לאיזשהו $P\mid p\mathcal{O}_L$ אידאל ראשוני של $\mathcal{O}_L$. בפרט,

$$\mathcal{F}_\theta\cap\mathbb{Z}\subseteq P\cap\mathbb{Z}=p\mathbb{Z}.$$

נשים לב כי $2\cdot\frac{1+\sqrt{d}}{2}=1+\sqrt{d}\in\mathbb{Z}\left[\sqrt{d}\right]=\mathbb{Z}[\theta]$, לכן $2\in\mathcal{F}_\theta$, כלומר $\mathcal{F}_\theta\cap\mathbb{Z}=2\mathbb{Z}$ (כבר ראינו כי $\mathcal{F}_\theta\neq\mathcal{O}_L$, לכן החיתוך לא יכול להיות כל $\mathbb{Z}$). אם כן, תנאי משפט 3.5 מתקיימים לכל $p\neq 2$, ונוכל לפעול בדומה לדוגמה הקודמת.

3.3 הסתעפות בהרחבות גלואה

כעת נניח שההרחבה L/K גלואה. לכל $\sigma \in \operatorname{Gal}(L/K)$, $\sigma(B) = B$ (כי לכל $x \in B$, $\sigma(x)$ שורש של אותו פולינום מינימלי, ובפרט σ שולח איברים שלמים מעל A לאיברים שלמים). יותר מזה, לכל $\mathfrak{p} \subseteq A$ ראשוני, $\sigma(\mathfrak{p}B) = \mathfrak{p}B$ מאותה הסיבה. נוסף על כך, לכל $P \subseteq B$ ראשוני, מושרה איזומורפיזם $\sigma : B/P \xrightarrow{\sim} B/\sigma(P)$, ולכן גם $\sigma(P)$ ראשוני.

לכן, אם $\mathfrak{p}B = P_1^{e_1} \dots P_r^{e_r}$, נקבל $\mathfrak{p}B = \sigma(\mathfrak{p}B) = \sigma(P_1)^{e_1} \dots \sigma(P_r)^{e_r}$. מכאן נקבל ש-$\sigma$ משרה תמורה על האידאלים הראשוניים $\mathfrak{p} \mid P$.

טענה 3.9. הפעולה של $\operatorname{Gal}(L/K)$ על הקבוצה $\{P \subseteq B : P : \mathfrak{p}\}$ הינה טרנזיטיבית.

הוכחה. יהי $\mathfrak{p}B = P_1^{e_1} \dots P_r^{e_r}$. נניח בשלילה שקיימים i, j כך ש-$\sigma(P_i) \neq P_j$ לכל $\sigma \in \operatorname{Gal}(L/K)$. לפי משפט השאריות הסיני, קיים $x \in B$ המקיים

$$\begin{cases} x \equiv 0 \pmod{P_j} \\ x \equiv 1 \pmod{\sigma(P_i)} \quad \forall \sigma \in \operatorname{Gal}(L/K) \end{cases}$$

מתקיים

$$\mathrm{N}_{L/K}(x) = \underbrace{x}_{\in P_j} \cdot \prod_{\sigma \neq \mathrm{id}} \sigma(x) \in P_j ,$$

ולכן

$$\mathrm{N}_{L/K}(x) \in A \cap P_j = \mathfrak{p} .$$

מצד שני, $x \notin \sigma(P_i)$ לכל i, לכן $\sigma(x) \notin P_i$ לכל i; מהראשוניות של P_i,

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in \operatorname{Gal}(L/K)} \sigma(x) \notin P_i .$$

אבל זו סתירה, כי הוכחנו $\mathrm{N}_{L/K}(x) \in \mathfrak{p} \subseteq \mathfrak{p}B \subseteq P_i$. □

מסקנה 3.10. תהי L/K הרחבת גלואה, יהי $\mathfrak{p} \subseteq A$ ראשוני, ויהי $\mathfrak{p}B = P_1^{e_1} \dots P_r^{e_r}$ הפירוק של $\mathfrak{p}$ לאידאלים ראשוניים מעל B. נזכור כי $f_i = [B/P_i : A/\mathfrak{p}]$. אזי

$$e_1 = \dots = e_r = e, \qquad f_1 = \dots = f_r = f .$$

לכן, הנוסחה היסודית מקבלת את הצורה

$$n = [L : K] = \sum_{i=1}^{r} e_i f_i = e \cdot f \cdot r .$$

הוכחה. לכל $1 \leq j \leq r$ קיים $\sigma \in \operatorname{Gal}(L/K)$ כך ש-$\sigma(P_1) = P_j$. אזי

$$P_1^{e_1} \dots P_r^{e_r} = \mathfrak{p}B = \sigma(\mathfrak{p}B) = \sigma(P_1)^{e_1} \dots \sigma(P_r)^{e_r} .$$

מיחידות הפירוק אפשר להשוות את החזקות של P_j; לכן $e_1 = e_j$. כיוון שזה נכון לכל j, נקבל $e_1 = \dots = e_r = e$.

מצד שני, σ משרה $\sigma : B/P_1 \xrightarrow{\sim} B/\sigma(P_1) = B/P_j$, והפעולה של σ שומרת את המבנה של החוגים כמרחבים וקטוריים מעל $A/\mathfrak{p}$. לכן האיזומורפיזם הנ"ל שומר את המימדים, כלומר $f_1 = f_j$. לכן $f_1 = \dots = f_r = f$. □

הערה. נניח $[L:\mathbb{Q}]=2$ (ובפרט $L/\mathbb{Q}$ גלואה). אזי $efr=2$, ולכן יש שלוש אפשרויות:

- $e=2,f=1,r=1$ - המקרה המסועף.
- $e=1,f=2,r=1$ - $p\mathcal{O}_L$ נשאר ראשוני, $\mathrm{N}\left(p\mathcal{O}_L\right)=p^2$.
- $e=1,f=1,r=2$ - $p\mathcal{O}_L$ מתפרק למכפלת שני אידאלים ראשוניים שונים, שניהם מנורמה p.

הגדרה 3.11. יהי $\mathfrak{p}\mid P$. נגדיר את **תת-חבורת הפירוק** (**decomposition subgroup**) להיות

$$G_P=\left\{\sigma\in\mathrm{Gal}\left(L/K\right):\sigma\left(P\right)=P\right\}.$$

הערה. לפי משפט מסלול-מייצב, $[G:G_P]=r$.

הגדרה 3.12. $\mathfrak{p}$ נקרא **אינרטי** (**inertial**) אם $\mathfrak{p}B$ ראשוני ב-B.

מסקנה 3.13.

א. $G_P=\mathrm{Gal}\left(L/K\right)\iff r=1\iff\mathfrak{p}B=P^e$, כלומר $\mathfrak{p}$ אינו מתפרק.

ב. $G_P=\{e\}\iff r=n\iff\mathfrak{p}B=P_1\ldots P_n$ כאשר ה-P_i-ים ראשוניים שונים ו-$B/P_i=A/\mathfrak{p}$, כלומר $\mathfrak{p}$ מתפרק לגמרי.

תרגיל 3.14. בהינתן מגדל הרחבות $K\subseteq L\subseteq M$ ואידאלים ראשוניים $\mathfrak{P}\subseteq P\subseteq\mathfrak{p}$, מתקיים

$$e\left(\mathfrak{P}/\mathfrak{p}\right)=e\left(\mathfrak{P}/P\right)\cdot e\left(P/\mathfrak{p}\right)$$

וכן

$$f\left(\mathfrak{P}/\mathfrak{p}\right)=f\left(\mathfrak{P}/P\right)\cdot f\left(P/\mathfrak{p}\right).$$

טענה 3.15. יהי Z שדה השבת של G_P, ויהי A_Z הסגור השלם של A ב-Z. נסמן $P_Z=A_Z\cap P\subseteq A_Z$. אזי:

א. P הינו האידאל הראשוני היחיד של B שמחלק את P_Z.

ב. $e\left(P/P_Z\right)=e\left(P/\mathfrak{p}\right)$, $f\left(P/P_Z\right)=f\left(P/\mathfrak{p}\right)$, ו-$e\left(P_Z/\mathfrak{p}\right)=f\left(P_Z/\mathfrak{p}\right)=1$.

הוכחה.

א. לכל $\sigma\in\mathrm{Gal}\left(L/Z\right)=G_P$, $\sigma\left(P\right)=P$. אך $\mathrm{Gal}\left(L/Z\right)$ פועלת טרנזיטיבית על $\{Q\subseteq B:Q\mid P_Z\}$.

ב. מצד אחד, $[L:Z]=|G_P|=\frac{n}{r}=e\left(P/\mathfrak{p}\right)\cdot f\left(P/\mathfrak{p}\right)$. מצד שני, לפי הנוסחה היסודית,

$$e\left(P/P_Z\right)\cdot f\left(P/P_Z\right)\cdot 1=[L:Z].$$

בגלל תרגיל 3.14, $e\left(P/P_Z\right)\mid e\left(P/\mathfrak{p}\right)$ ו-$f\left(P/P_Z\right)\mid f\left(P/\mathfrak{p}\right)$. בסך הכל נקבל את השוויונות הדרושים.

□

הגדרה 3.16. יהי A תחום דדקינד ו-$\mathfrak{p} \subseteq A$ אידאל ראשוני בו. המנה $A/\mathfrak{p}$ נקראת **שדה השארית (residue field)** של A ביחס ל-$\mathfrak{p}$. אם $K = \mathrm{Frac} A$, נהוג לסמן את שדה השארית של A ב-k.

נקבע $\mathfrak{p} \mid P$. נסמן $k = A/\mathfrak{p}$ ו-$\ell = B/P$. כל $\sigma \in G_P$ מגדיר $\sigma : B \xrightarrow{\sim} B$ שקובע את P, ולכן הוא משרה $\sigma : \ell \to \ell$ שקובע כל איבר של k.

טענה 3.17. נניח שההרחבה ℓ/k ספרבילית. אזי היא גלואה, ומקבלים העתקה טבעית $G_P \to \mathrm{Gal}(\ell/k)$. נוסף על כך, ההעתקה הזו היא על.

הוכחה. ℓ/k סופית וספרבילית, לכן פרימיטיבית. יהי $\overline{\theta} \in \ell$ איבר יוצר של ההרחבה, כלומר $\ell = k(\overline{\theta})$. תהי $\theta \in B$ הרמה של $\overline{\theta}$, יהי $\overline{g}(x) \in k[x]$ הפולינום המינימלי של $\overline{\theta}$, ויהי $f(x) \in A[x]$ הפולינום המינימלי של θ. $f(\theta) = 0$, לכן $\overline{f}(\overline{\theta}) = 0$, כלומר $\overline{g} \mid \overline{f}$.

L/K הרחבה נורמלית, ומכאן ש-$f(x)$ מתפרק למכפלה של גורמים לינאריים ב-$B[x]$, ובפרט $\overline{f}(x)$ (ולכן גם $\overline{g}(x)$) מתפרק למכפלה של גורמים לינאריים ב-$\ell[x]$. זה מראה ש-ℓ/k נורמלית, כלומר גלואה.

נוכיח שההעתקה $\varphi : G_P \to \mathrm{Gal}(\ell/k)$ היא על. יהי $\overline{\sigma} \in \mathrm{Gal}(\ell/k)$, ונרצה למצוא הרמה $\sigma \in G_P$ של $\overline{\sigma}$. בלי הגבלת הכלליות, אפשר להניח ש-$G_P = \mathrm{Gal}(L/K)$; אכן, אם נחליף את K ב-Z,

$$[B/P : A/\mathfrak{p}] = [B/P : A_Z/P_Z]$$

ונקבל $A_Z/P_Z = k$ – כלומר $\mathrm{Gal}(\ell/k)$ לא תשתנה.

$\overline{\sigma}(\overline{\theta})$ הינו צמוד של $\overline{\theta}$, כלומר שורש של $\overline{g}(x)$, ובפרט שורש של $\overline{f}(x)$. לכן ניתן להרים אותו לשורש η של $f(x)$. אבל L/K, ולכן קיים $\sigma \in \mathrm{Gal}(L/K)$ כך ש-$\sigma(\theta) = \eta$. לכן

$$\varphi(\sigma)(\overline{\theta}) = \overline{\eta} = \overline{\sigma}(\overline{\theta}).$$

כיוון ש-$\overline{\theta}$ איבר פרימיטיבי, $\varphi(\sigma) = \overline{\sigma}$. לכן φ על. □

הגדרה 3.18. **תת-חבורת ההתמדה (inertia subgroup)** של P הינה

$$I_P = \ker(G_P \twoheadrightarrow \mathrm{Gal}(\ell/k))$$

הערה. $f = f(P/\mathfrak{p}) = [\ell : k] = |\mathrm{Gal}(\ell/k)|$, לכן $e = \frac{|G_P|}{f} = |I_P|$. כלומר, $I_P = \{e\}$ אם ורק אם $\mathfrak{p}$ אינו מסועף ב-L.

3.4 השדות הציקלוטומיים

הגדרה 3.19. **שדה ציקלוטומי (cyclotomic field)** הינו שדה מהצורה $K = \mathbb{Q}(\zeta_n)$, כאשר ζ_n שורש n-י פרימיטיבי של היחידה.

הערה. $[K : \mathbb{Q}] = \varphi(n)$.

נרצה להבין כיצד מתפרק האידאל $p\mathcal{O}_K$ לאידאלים ראשוניים.

טענה 3.20. יהי $n = p^a$. אזי האידאל הראשי $\mathfrak{p} = (1 - \zeta_n)\mathcal{O}_K$ ראשוני, ומתקיים $p\mathcal{O}_K = \mathfrak{p}^{\varphi(n)}$. בפרט,

$$\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$$

(כלומר $f = 1$).

הוכחה. הפולינום המינימלי של ζ_{p^a} הוא

$$\Phi_{p^a}(x) = \frac{1-x^{p^a}}{1-x^{p^{a-1}}} = 1 + x^{p^{a-1}} + \cdots + x^{p^{(p-1)p^{a-1}}}.$$

נציב $x=1$, ונקבל

$$\prod_{c\in(\mathbb{Z}/p^a\mathbb{Z})^\times} \left(1-\zeta_{p^a}^c\right) = \Phi_{p^a}(1) = p \qquad (\star).$$

כעת נטען כי כל האיברים $1-\zeta_{p^a}^c$ מייצרים את אותו אידאל ראשי של $\mathcal{O}_K$. אכן,

$$1-\zeta_{p^a}^c = \left(1-\zeta_{p^a}\right)\underbrace{\left(1+\zeta_{p^a}+\cdots+\zeta_{p^a}^{c-1}\right)}_{u}.$$

נוכיח ש-$u\in\mathcal{O}_K^\times$: יהי c' כך ש-$cc'\equiv 1 \pmod{p^a}$. אזי

$$1-\zeta_{p^a} = 1-\zeta_{p^a}^{cc'} = \left(1-\zeta_{p^a}^c\right)\underbrace{\left(1+\zeta_{p^a}^c+\cdots+\zeta_{p^a}^{(c'-1)c}\right)}_{u'}.$$

לכן

$$1-\zeta_{p^a} = uu'\left(1-\zeta_{p^a}\right),$$

כלומר $uu'=1$. לכן כל האיברים הנ"ל מייצרים את אותו אידאל ראשי $\mathfrak{p}$, ומכאן

$$p\mathcal{O}_K = \mathfrak{p}^{\varphi(p^a)}.$$

$\mathfrak{p}$ ראשוני כי $\mathrm{N}(\mathfrak{p}) = p$ (לפי $(\star)$). לכן זהו הפירוק של $p\mathcal{O}_K$ מעל $\mathcal{O}_K$. $\square$

תרגיל 3.21. נתבונן בבסיס $\left\{\zeta_n^c : c\in(\mathbb{Z}/n\mathbb{Z})^\times\right\}$ של K מעל $\mathbb{Q}$. אם $n=p^a$, אזי

$$\mathrm{d}_{K/\mathbb{Q}}\left(\zeta_n^c : c\in(\mathbb{Z}/n\mathbb{Z})^\times\right) = \pm p^{p^{a-1}(ap-a-1)}.$$

טענה 3.22. לכל $n\in\mathbb{Z}$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

הוכחה. נתחיל מהמקרה שבו $n=p^a$. לפי הטענה הקודמת,

$$\mathcal{O}_K/(1-\zeta_n)\mathcal{O}_K \cong \mathbb{Z}/p\mathbb{Z}.$$

לכן אפשר לקחת את $0,1,\ldots,p-1$ כנציגים של כל המחלקות. זה אומר שאם $\pi = 1-\zeta_n$,

$$\mathcal{O}_K = \mathbb{Z}+\pi\mathcal{O}_K,$$

ובפרט

$$\mathcal{O}_K = \mathbb{Z}[\zeta_n]+\pi\mathcal{O}_K.$$

לכן

$$\pi\mathcal{O}_K = \pi\mathbb{Z}[\zeta_n]+\pi^2\mathcal{O}_K,$$

ואפשר להמשיך לפתח ולקבל

$$\mathcal{O}_K=\mathbb{Z}\left[\zeta_n\right]+\pi\mathbb{Z}\left[\zeta_n\right]+\pi^2\mathcal{O}_K=\mathbb{Z}\left[\zeta_n\right]+\pi^2\mathcal{O}_K.$$

אם ממשיכים באינדוקציה, מקבלים שלכל $m\in\mathbb{N}$ מתקיים $\mathcal{O}_K=\mathbb{Z}\left[\zeta_n\right]+\pi^m\mathcal{O}_K$. אבל אנחנו יודעים ש-$\bigcap_{m=0}^{\infty}\pi^m\mathcal{O}_K=0$, לכן $\mathcal{O}_K=\mathbb{Z}\left[\zeta_n\right]$.

נעבור למקרה הכללי. נשתמש בלמה הבאה:

למה. תהיינה K,L הרחבות של $\mathbb{Q}$, ונניח שהדיסקרימיננטות $\mathrm{d}_{K/\mathbb{Q}}$ ו-$\mathrm{d}_{L/\mathbb{Q}}$ זרות. יהיו $\alpha_1,\ldots,\alpha_m$ ו-$\beta_1,\ldots,\beta_n$ בסיסים שלמים של K ושל L בהתאמה. אזי

$$\left\{\alpha_i\beta_j:1\leq i\leq m,1\leq j\leq n\right\}$$

בסיס שלם של הקומפוזיטום KL.

הוכחה. תרגיל בית. □

יהי $n=p_1^{a_1}\ldots p_r^{a_r}$ כלשהו; אז מתקיים

$$\mathbb{Q}\left(\zeta_n\right)=\mathbb{Q}\left(\zeta_{p_1^{a_1}}\right)\ldots\mathbb{Q}\left(\zeta_{p_r^{a_r}}\right).$$

לפי תרגיל 3.21, הדיסקרימיננטות כולן זרות, ולכל i הקבוצה

$$\left\{\zeta_{p_i^{a_i}}^c:c\in\left(\mathbb{Z}/p_i^{a_i}\mathbb{Z}\right)^\times\right\}$$

היא בסיס שלם של $\mathbb{Q}\left(\zeta_{p_i^{a_i}}\right)$. לכן יש בסיס שלם של $\mathbb{Q}\left(\zeta_n\right)$ שמוכל ב-$\mathbb{Z}\left[\zeta_n\right]$, מה שמראה $\mathcal{O}_{\mathbb{Q}(\zeta_n)}\subseteq\mathbb{Z}\left[\zeta_n\right]$. מצד שני, $\mathbb{Z}\left[\zeta_n\right]$ הרחבה שלמה של $\mathbb{Z}$, ולכן יש שוויון. □

טענה 3.23. יהי $n=\prod_p p^{a_p}$ (כאשר $a_p=0$ לכמעט כל p). יהי p מספר ראשוני, ויהי $f_p\geq 1$ המספר הטבעי הקטן ביותר המקיים

$$p^{f_p}\equiv 1\pmod{\frac{n}{p^{a_p}}}.$$

אזי

$$p\mathcal{O}_{\mathbb{Q}(\zeta_n)}=\left(P_1\ldots P_r\right)^{\varphi\left(p^{a_p}\right)},$$

ובנוסף $f=\left[{}^{p\mathbb{Q}(\zeta_n)}/_{P_i}:\mathbb{F}_p\right]=f_p$. מהנוסחה היסודית, $r=\frac{\varphi(n)}{\varphi\left(p^{a_p}\right)\cdot f_p}$.

הוכחה. נרשום $K=\mathbb{Q}\left(\zeta_n\right)$. נתחיל מהמקרה שבו $a_p=0$, כלומר $p\nmid n$. לפי טענה 3.22, $\mathcal{O}_K=\mathbb{Z}\left[\zeta_n\right]$, ולכן $\mathcal{F}_{\zeta_n}=\mathcal{O}_K=\mathbb{Z}\left[\zeta_n\right]$. מכאן מספיק לפרק את הפולינום המינימלי של ζ_n, כלומר את $\Phi_n\left(x\right)$, מודולו p. יהי $f\left(x\right)=x^n-1$. $f'\left(x\right)=nx^{n-1}$, לכן לפולינומים $f\left(x\right)$ ו-$f'\left(x\right)$ אין שורשים משותפים בשדה ${}^{\mathcal{O}_K}/_P$ לכל $P\mid p\mathcal{O}_K$. מכאן שהשדה ${}^{\mathcal{O}_K}/_P$ מכיל n שורשים n-ים שונים של 1.

ההרחבה המינימלית של $\mathbb{F}_p$ המכילה n שורשים שונים של 1 היא $\mathbb{F}_{p^{f_p}}$. מודולו p, מתקיים

$$\Phi_n\left(x\right)=\prod_{c\in\left(\mathbb{Z}/n\mathbb{Z}\right)^\times}\left(x-\zeta_n^c\right)=\prod\left(\text{minimal polynomials of the elements of}\,\mathbb{F}_{p^{f_p}}\right)\pmod p$$

זה אומר ש-$\overline{\Phi_n}(x) = \overline{g_1}(x) \dots \overline{g_r}(x)$ כאשר $\deg \overline{g_i} = f_p$ וה-$\overline{g_i}(x)$-ים כולם זרים. לפי משפט 3.5, $p\mathcal{O}_K = P_1 \dots P_r$ כאשר $P_i = (p, g_i(\zeta_n))$ ו-$f = f_p$.

כעת נניח $a_p > 0$. במקרה הזה נכתוב $n = p^{a_p} \cdot m$ (כאשר m זר ל-p), ואז

$$K = \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_{p^{a_p}}).$$

מתקיים

$$\Phi_n(x) = \prod_{c \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^c) = \prod_{\substack{d \in (\mathbb{Z}/m\mathbb{Z})^\times \\ d' \in (\mathbb{Z}/p^{a_p}\mathbb{Z})^\times}} \left(x - \zeta_m^d \zeta_{p^{a_p}}^{d'}\right).$$

אם מסתכלים מודולו p,

$$x^{p^{a_p}} - 1 \equiv (x-1)^{p^{a_p}} \pmod p \Longrightarrow \zeta_{p^{a_p}} \equiv 1 \pmod{p\mathcal{O}_K}.$$

לכן

$$\Phi_n(x) = (\Phi_m(x))^{\varphi(p^{a_p})} \pmod p.$$

נקבל את אותו הפירוק כמו קודם, רק שהפעם כל הגורמים יופיעו בחזקת $\varphi(p^{a_p})$, כמבוקש.
□

4 הערכות (ולואציות)

4.1 שדות עם הערכה

הגדרה 4.1. יהי K שדה. **הערכה (כפלית)** על K הינה פונקציה $|\cdot| : K \to \mathbb{R}$ המקיימת את התכונות הבאות:

א. $|x| \geq 0$ לכל $x \in K$. בנוסף, $|x| = 0 \iff x = 0$.

ב. $|xy| = |x| \cdot |y|$ לכל $x, y \in K$.

ג. $|x+y| \leq |x| + |y|$ לכל $x, y \in K$.

דוגמה 4.2.

א. $K = \mathbb{R}, \mathbb{C}$ עם הערך המוחלט הרגיל.

ב. יהי K שדה כלשהו. **ההערכה הטריוויאלית** על K היא $|x| = \begin{cases} 0, & x = 0 \\ 1, & x \neq 0 \end{cases}$.

ג. ניקח $K = \mathbb{Q}$, p ראשוני כלשהו. **ההערכה ה-p-אדית** מוגדרת כך: אם $0 \neq x = \frac{m}{n} = p^c \cdot \frac{m'}{n'}$ עבור m', n' זרים ל-p ו-$c \in \mathbb{Z}$, נגדיר $|x|_p = \left(\frac{1}{p}\right)^c$. אם $x = 0$, נגדיר $|x|_p = 0$.

למעשה, ההערכה ה-p-אדית מקיימת תנאי חזק יותר מאי-שוויון המשולש:

$$|x+y|_p \leq \max\left\{|x|_p, |y|_p\right\}.$$

כל הערכה $|\cdot|$ על K משרה מבנה של מרחב מטרי על K לפי $d(x,y) = |x-y|$, ולכן מקבלים טופולוגיה מטרית.

הגדרה 4.3. שתי הערכות על K נקראות **שקולות** אם הן מגדירות את אותה טופולוגיה.

טענה 4.4. תהיינה $|\cdot|_1$ ו-$|\cdot|_2$ שתי הערכות לא-טריוויאליות על K. $|\cdot|_1$ ו-$|\cdot|_2$ שקולות אם ורק אם קיים $s>0$ כך שלכל $x\in K$, $|x|_2=|x|_1^s$.

הוכחה. $\boxed{\Rightarrow}$ אם קיים s כזה,

$$\{y\in K:|y-x|_2<\varepsilon\}=\left\{y\in K:|y-x|_1<\varepsilon^{1/s}\right\}.$$

במילים אחרות שתי ההערכות מגדירות את אותם הכדורים הפתוחים, ולכן את אותה הטופולוגיה.

$\boxed{\Leftarrow}$ נניח שההערכות נותנות את אותה הטופולוגיה. נשים לב ש-$|x|_i<1$ אם ורק אם הסדרה $1,x,x^2,\dots$ מתכנסת ל-0 לפי הטופולוגיה של $|\cdot|_i$. לכן,

$$\{x\in K:|x|_1<1\}=\{x\in K:|x|_2<1\}.$$

יהי $y\in K$ כך ש-$|y|_i>1$ (קיים y כזה, כיוון שההערכה אינה טריוויאלית), ויהי $x\in K^\times$. קיים $\alpha\in\mathbb{R}$ כך ש-$|x|_1=|y|_1^\alpha$. תהי $\left\{\frac{m_i}{n_i}\right\}$ סדרה יורדת של מספרים רציונליים ששואפת ל-α. אזי

$$\begin{aligned}|x|_1&<|y|_1^{\frac{m_i}{n_i}}\\ |x^{n_i}|_1&<|y^{m_i}|_1\\ \left|\frac{x^{n_i}}{y^{m_i}}\right|_1&<1\\ \left|\frac{x^{n_i}}{y^{m_i}}\right|_2&<1\\ |x^{n_i}|_2&<|y^{m_i}|_2\\ |x|_2&<|y|_2^{\frac{m_i}{n_i}}\end{aligned}$$

זה נכון לכל i, ולכן $|x|_2\le|y|_2^\alpha$. אם ניקח סדרה עולה של מספרים רציונליים ששואפת ל-α, נקבל כי $|x|_2\ge|y|_2^\alpha$; בסך הכל,

$$\frac{\log|x|_1}{\log|y|_1}=\alpha=\frac{\log|x|_2}{\log|y|_2}.$$

לכן לכל $x\in K^\times$

$$\frac{\log|x|_1}{\log|x|_2}=\frac{\log|y|_1}{\log|y|_2}=s>0$$

קבוע. זה בדיוק מראה ש-$|x|_1=|x|_2^s$, כנדרש. $\square$

הגדרה 4.5. הערכה $|\cdot|$ נקראת **לא ארכימדית** אם $\{|n|:n\in\mathbb{N}\}$ חסומה. הערכה שאינה לא ארכימדית נקראת **ארכימדית**.

טענה 4.6. הערכה $|\cdot|$ היא לא ארכימדית אם ורק אם היא מקיימת את אי-שוויון המשולש החזק:

$$|x+y|\le\max\{|x|,|y|\}.$$

הוכחה. $\boxed{\Rightarrow}$ $|1| = 1$ כי $x \cdot 1 = x$ לכל $x \in K$. נקבל $|2| = |1+1| \leq \max\{|1|, |1|\} = 1$. באינדוקציה, $|n| \leq 1$ לכל $n \in \mathbb{N}$.

$\boxed{\Leftarrow}$ נניח שקיים M כך ש-$|n| \leq M$ לכל $n \in \mathbb{N}$. יהיו $x, y \in K$, ונניח $|y| \leq |x|$. מתקיים

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i},$$

ולכן

$$|x+y|^n = \left|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\right| \leq \sum_{i=0}^{n} \left|\binom{n}{i}\right| \cdot |x|^i \cdot |y|^{n-i} \leq \sum_{i=0}^{n} M \cdot |x|^i \cdot |x|^{n-i} = $$
$$= M \cdot |x|^n \cdot (n+1)$$

כלומר

$$|x+y| \leq (n+1)^{1/n} \cdot M^{1/n} \cdot |x|$$

אם נשאיף $n \to \infty$, נקבל $|x+y| \leq |x| = \max\{|x|, |y|\}$. □

טענה 4.7. תהי $|\cdot|$ הערכה על K.

א. אם $|\cdot|$ לא ארכימדית, $|n| \leq 1$ לכל $n \in \mathbb{N}$.

ב. אם $|\cdot|$ ארכימדית, $|n| \geq 1$ לכל $n \in \mathbb{N}$.

הוכחה. את המקרה הלא ארכימדי הוכחנו בטענה הקודמת; לכן נניח ש-$|\cdot|$ ארכימדית. נניח בשלילה שקיים $n \in \mathbb{N}$ שעבורו $|n| < 1$. כל $m \in \mathbb{N}$ ניתן לרשום באופן

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

כאשר $a_i \in \{0, 1, \ldots, n-1\}$. לפי אי-שוויון המשולש ואינדוקציה, $|k| \leq k$ לכל $k \in \mathbb{N}$. מכאן

$$|m| \leq |a_0| + |a_1| \cdot |n| + \cdots + |a_r| \cdot |n|^r \leq (n-1) \sum_{i=0}^{r} |n|^i < (n-1) \sum_{i=0}^{\infty} |n|^i = \frac{n-1}{1-|n|}$$

בסתירה לארכימדיות. □

טענה 4.8. תהי $|\cdot|$ הערכה לא ארכימדית. אם $|y| \neq |x|$, אזי $|x+y| = \max\{|x|, |y|\}$.

הוכחה. נניח $|y| < |x|$. אזי

$$|x| = |(x+y) - y| \leq \max\{|x+y|, |y|\} = |x+y|,$$

אך לפי אי-שוויון המשולש החזק, $|x+y| \leq |x|$. לכן $|x+y| = |x|$. □

כעת אנחנו יכולים להוכיח את משפט אוסטרובסקי, שממיין את כל ההערכות על $\mathbb{Q}$.

משפט 4.9 (משפט אוסטרובסקי). כל הערכה לא-טריוויאלית על $\mathbb{Q}$ שקולה להערכה הרגילה $|\cdot|_\infty$ או להערכה ה-p-אדית $|\cdot|_p$ לאיזשהו ראשוני p.

הוכחה. תהי $|\cdot|$ הערכה לא ארכימדית על $\mathbb{Q}$. כיוון שההערכה לא-טריוויאלית, קיים $n \in \mathbb{N}$ כך ש-$|n| < 1$. לכן קיים ראשוני p כך ש-$|p| < 1$ (אחד הגורמים של n). נשים לב שהקבוצה $I = \{m \in \mathbb{Z} : |m| < 1\}$ היא אידאל של $\mathbb{Z}$, והיא אידאל אמיתי כי $|1| = 1$. לכן $I = p\mathbb{Z}$. זה אומר שאם $0 \neq x = p^c \cdot \frac{m'}{n'} \in \mathbb{Q}$ כאשר $p \nmid m', n'$,

$$|x| = |p|^c \cdot \frac{|m'|}{|n'|} = |p|^c = \left(\frac{1}{p}\right)^{-c\log_p|p|} = |x|_p^{-\log_p|p|} \text{ .}$$

מכאן ש-$|\cdot|$ שקולה ל-$|\cdot|_p$.

כעת נניח כי $|\cdot|$ ארכימדית, ויהיו $m, n \in \mathbb{N}$. נרשום את m בבסיס n:

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

כאשר $a_i \in \{0, 1, \ldots, n-1\}$ ו-$a_r \neq 0$. נזכור שלכל $b \in \mathbb{N}$, $|b| \le b$ מאי-שוויון המשולש. כיוון ש-$n^r \le m$, $r \le \log_n m = \frac{\log m}{\log n}$. לפי אי-שוויון המשולש,

$$|m| \le \sum_{i=0}^{r} |a_i| \cdot |n|^i \le \sum_{i=0}^{r} |a_i| \cdot |n|^r \le \sum_{i=0}^{r} n \cdot |n|^r = n\,(r+1)\,|n|^r \le$$
$$\le n \cdot \left(1 + \frac{\log m}{\log n}\right) \cdot |n|^{\frac{\log m}{\log n}}$$

אם נחליף את m ב-m^k,

$$|m|^k = \left|m^k\right| \le n \cdot \left(1 + \frac{k\log m}{\log n}\right) \cdot |n|^{\frac{k\log m}{\log n}}$$

ונקבל שלכל $k \ge 1$,

$$|m| \le n^{1/k} \cdot \left(1 + \frac{k\log m}{\log n}\right)^{1/k} \cdot |n|^{\frac{\log m}{\log n}} \text{ .}$$

נשאיף $k \to \infty$, ונקבל

$$|m| \le |n|^{\frac{\log m}{\log n}} \Longrightarrow |m|^{\frac{1}{\log m}} \le |n|^{\frac{1}{\log n}} \text{ .}$$

אם נחליף תפקידים בין m ל-n, נקבל $|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log n}}$. נגדיר

$$s = \log |n|^{\frac{1}{\log n}} = \frac{\log|n|}{\log n} > 0$$

(בלתי-תלוי ב-n), ולכן $|n|_\infty^s = n^{\frac{\log|n|}{\log n}} = n^{\log_n|n|} = |n|$.

הראינו שלכל $n \in \mathbb{N}$, $|n|_\infty^s = |n|$; לכן זה נכון לכל $x \in \mathbb{Q}$, כנדרש. □

4.2 ההשלמה של שדה ביחס להערכה

הגדרה 4.10. יהי K שדה עם הערכה לא-טריוויאלית. סדרה $\{a_n\}_{n=1}^\infty$ של איברים מ-K נקראת **סדרת קושי**, אם לכל $\varepsilon > 0$ קיים N כך שלכל $m, n \ge N$ מתקיים $|a_m - a_n| < \varepsilon$.

סדרה $\{a_n\}_{n=1}^\infty$ נקראת **אפסה**, אם לכל $\varepsilon > 0$ קיים N כך שלכל $n \ge N$ מתקיים $|a_n| < \varepsilon$.

טענה 4.11. הקבוצה R של כל סדרות קושי של איברים מ-K, עם חיבור וכפל איבר-איבר, הינה חוג. בנוסף, תת-הקבוצה I של הסדרות האפסות הינה אידאל מקסימלי של R.

הגדרה 4.12. נגדיר $\widehat{K} = {}^{R}/_{I}$. זהו שדה, וכן $K \hookrightarrow \widehat{K}$ לפי $x \mapsto (x, x, \dots)$. $\widehat{K}$ נקרא **ההשלמה** של K ביחס ל-$|\cdot|$.

דוגמה 4.13. עבור $K = \mathbb{Q}$ עם ההערכה הרגילה $|\cdot|_\infty$, $\widehat{K} = \mathbb{R}$.

הגדרה 4.14. ההשלמה של $\mathbb{Q}$ ביחס ל-$|\cdot|_p$ נקראת **שדה המספרים ה-p-אדיים**, ומסומנת $\mathbb{Q}_p$.

הגדרה 4.15. שדה עם הערכה $|\cdot|$ נקרא **שלם**, אם לכל סדרת קושי יש גבול ב-K.

טענה 4.16. יהי K שדה עם הערכה לא ארכימדית $|\cdot|$.

א. לכל x, יהי $B_\varepsilon(x) = \{y \in K : |y - x| < \varepsilon\}$. אז לכל $y \in B_\varepsilon(x)$ מתקיים $B_\varepsilon(x) = B_\varepsilon(y)$.

ב. טור $\sum_{k=1}^{\infty} a_k$ מתכנס (כלומר סדרת הסכומים החלקיים היא סדרת קושי) אם ורק אם הסדרה a_k אפסה.

הוכחה.

א. תהי $z \in B_\varepsilon(x)$. אזי $|x - y| < \varepsilon$, $|x - z| < \varepsilon$, ולכן

$$|y - z| = |(x - z) - (x - y)| \le \max\{|x - z|, |x - y|\} < \varepsilon,$$

כלומר $B_\varepsilon(x) \subseteq B_\varepsilon(y)$. מסימטריה, נקבל שוויון.

ב. $\boxed{\Leftarrow}$ כמו באינפי 1.
$\boxed{\Rightarrow}$ יהי $\varepsilon > 0$. לכן קיים N כך ש-$|a_k| < \varepsilon$ לכל $k \ge N$. אזי לכל $p \ge 0$ ו-$k \ge N$,

$$|a_k + \dots + a_{k+p}| \le \max\{|a_k|, \dots, |a_{k+p}|\} < \varepsilon.$$

לכן סדרת הסכומים החלקיים הינה סדרת קושי.

□

מסקנה 4.17. הטופולוגיה המטרית על K היא בלתי-קשירה לחלוטין, כלומר לכל $x \neq y$ קיימות קבוצות סגורות וזרות U, V כך ש-$x \in U$ ו-$y \in V$.

הוכחה. לפי סעיף א' מהטענה הקודמת, שני כדורים פתוחים מאותו הרדיוס שווים או זרים זה לזה. זה אומר שמתקיים

$$B_\varepsilon(x) = K \setminus \bigcup_{y \notin B_\varepsilon(x)} B_\varepsilon(y).$$

אך איחוד של כדורים פתוחים הוא פתוח, ולכן כל כדור פתוח הוא סגור.
אם $\varepsilon = \frac{|x-y|}{2}$, אפשר לקחת $U = B_\varepsilon(x)$ ו-$V = B_\varepsilon(y)$. □

טענה 4.18. יהי K שדה עם הערכה $|\cdot|$, ותהי $\{a_n\}_{n=1}^{\infty}$ סדרת קושי. אזי הסדרה $\{|a_n|\}_{n=1}^{\infty}$ של מספרים ממשיים היא סדרת קושי.

לכן אפשר לכל $x \in \widehat{K}$ להגדיר $|x| = \lim_{n\to\infty} |a_n|$, כאשר $a_1, a_2, \dots$ סדרת קושי במחלקה של x.

דוגמה 4.19. ניקח $K = \mathbb{Q}$, $|\cdot| = |\cdot|_p$. אזי $|x|_p \in \{0\} \cup p^{\mathbb{Z}}$. לכן אם $\{a_n\}_{n=1}^{\infty}$ סדרת קושי לא אפסה, הסדרה $\left\{|a_n|_p\right\}_{n=1}^{\infty}$ מתייצבת. מכאן שאם $x \in \mathbb{Q}_p^\times$, $|x|_p \in p^{\mathbb{Z}}$.

4.3 חוג השלמים, שדה השאריות והלמה של הנזל

הגדרה 4.20. יהי K שדה עם הערכה לא ארכימדית $|\cdot|$.

א. הקבוצה $\mathcal{O} = \{x \in K : |x| \leq 1\}$ הינה חוג. זהו **חוג השלמים** של K.

ב. הקבוצה $\mathfrak{p} = \{x \in K : |x| < 1\}$ הינה אידאל של $\mathcal{O}$.

הערה 4.21. אם $x \in \mathcal{O} \setminus \mathfrak{p}$, אזי $x^{-1} \in K$ מקיים $\left|x^{-1}\right| = \frac{1}{|x|} = 1$, כלומר $x^{-1} \in \mathcal{O}$; לכן, $\mathcal{O}$ הוא חוג מקומי שהאידאל המקסימלי היחיד שלו הוא $\mathfrak{p}$.

הגדרה 4.22. השדה $k = \mathcal{O}/\mathfrak{p}$ נקרא **שדה השאריות (residue field)** של $\mathcal{O}$ (או של K).

הגדרה 4.23. הערכה לא ארכימדית $|\cdot|$ על שדה K נקראת **בדידה (discrete)**, אם

$$\max\{|x| : |x| < 1\}$$

קיים.

דוגמה 4.24. $|\cdot|_p$ על $\mathbb{Q}$ (או על $\mathbb{Q}_p$) בדידה, כי המקסימום הוא $\frac{1}{p}$.

הגדרה 4.25. יהי K שדה עם הערכה בדידה. איבר $\pi \in K$ כך ש-$|\pi| = \max\{|x| : |x| < 1\}$ נקרא **מאחד / אוניפורמיזנטה (uniformizer)**.

טענה 4.26. יהי K שדה עם הערכה בדידה.

א. $\mathfrak{p} = \pi\mathcal{O}$; כלומר $\mathfrak{p}$ אידאל ראשי.

ב. כל $x \in K^\times$ ניתן לרשום באופן יחיד בצורה $x = u \cdot \pi^n$ עבור $n \in \mathbb{Z}$ ו-$u \in \mathcal{O}^\times$.

הוכחה.

א. יהי $x \in \mathfrak{p}$. אזי

$$|x| \leq |\pi| \Longrightarrow \left|\frac{x}{\pi}\right| \leq 1 \Longrightarrow \frac{x}{\pi} \in \mathcal{O} \Longrightarrow x \in \pi\mathcal{O}\,.$$

ב. יהי $x \in \mathcal{O}$. אם $|x| = 1$, אז $x = u$ הפיך וסיימנו. לכן נניח $0 < |x| < 1$. קיים $n \geq 1$ (יחיד) שעבורו

$$|\pi|^{n+1} < |x| \leq |\pi|^n\,.$$

אם $|x| < |\pi|^n$, נקבל $|\pi| < \left|\frac{x}{\pi^n}\right| < 1$, בסתירה להגדרת π. לכן $|x| = |\pi|^n$, כלומר $u = \frac{x}{\pi^n}$ מקיים $|u| = 1$ – ומכאן ש-$u \in \mathcal{O}^\times$, כנדרש.

נותר המקרה שבו $x \notin \mathcal{O}$. אז $x^{-1} \in \mathcal{O}$. לפי המקרה הקודם, $x^{-1} = u \cdot \pi^n$ (עבור $n \geq 0$), לכן $x = u^{-1} \cdot \pi^{-n}$.

□

מסקנה 4.27. האידאלים הלא-אפסיים היחידים של $\mathcal{O}$ הם $\pi^n\mathcal{O} = \mathfrak{p}^n$.

הגדרה 4.28. חוג מקומי $\mathcal{O}$ עם אידאל מקסימלי $\mathfrak{p}$ נקרא **שלם ביחס לטופולוגיה ה-$\mathfrak{p}$-אדית**, אם לכל סדרה $\{a_n\}_{n=1}^\infty \subseteq \mathcal{O}$ המקיימת שלכל r קיים N כך שלכל $m, n \geq N$, $a_m \equiv a_n \pmod{\mathfrak{p}^r}$, קיים גבול $L \in \mathcal{O}$ (כלומר לכל r קיים N כך שלכל $n \geq N$, $a_n \equiv L \pmod{p^r}$).

דוגמה 4.29. יהי K שדה עם הערכה בדידה, ויהיו $\mathcal{O}$ ו-$\mathfrak{p}$ כנ"ל. אזי $\mathcal{O}$ שלם ביחס לטופולוגיה ה-$\mathfrak{p}$-אדית אם ורק אם K שלם ביחס ל-$|\cdot|$.
אכן, אם $\varepsilon = |\pi|^r$, נקבל

$$a_m \equiv a_n \pmod{\mathfrak{p}^r} \iff |a_m - a_n| < \varepsilon.$$

משפט 4.30 (למת הנזל). יהי $\mathcal{O}$ חוג מקומי שלם ביחס לטופולוגיה ה-$\mathfrak{p}$-אדית. יהי $k = \mathcal{O}/\mathfrak{p}$ שדה השאריות, יהי $f(x) \in \mathcal{O}[x]$, ותהי $\overline{f}(x) \in k[x]$ הרדוקציה של $f(x)$ מודולו $\mathfrak{p}$. נניח כי $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$, כאשר $\overline{g}(x), \overline{h}(x)$ פולינומים זרים ב-$k[x]$. אזי קיימים פולינומים $g(x), h(x) \in \mathcal{O}[x]$ שעבורם:

א. $f(x) = g(x) \cdot h(x)$.

ב. הרדוקציות של $g(x)$ ו-$h(x)$ מודולו $\mathfrak{p}$ הן $\overline{g}(x)$ ו-$\overline{h}(x)$.

ג. $\deg g(x) = \deg \overline{g}(x)$.

הוכחה. תהיינה $g_0(x), h_0(x) \in \mathcal{O}[x]$ הרמות כלשהן של $\overline{g}(x), \overline{h}(x)$ כך ש-$\deg g_0(x) = \deg \overline{g}(x)$. לכן

$$f(x) \equiv g_0(x) h_0(x) \pmod{\mathfrak{p}}.$$

נבנה באופן אינדוקטיבי סדרות של פולינומים $g_n(x), h_n(x) \in \mathcal{O}[x]$ כך שיתקיים:

$$f(x) \equiv g_n(x) h_n(x) \pmod{\mathfrak{p}^{n+1}},$$
$$g_n(x) \equiv g_{n-1}(x) \pmod{\mathfrak{p}^n},$$
$$h_n(x) \equiv h_{n-1}(x) \pmod{\mathfrak{p}^n},$$
$$\deg g_n(x) = \deg \overline{g}(x).$$

למה זה עוזר? נניח שמצאנו סדרות כאלו. כיוון ש-$g_n(x) \equiv g_{n-1}(x) \pmod{\mathfrak{p}^n}$, החל מהצעד ה-$n$-י המקדמים של x^k ב-$g_n(x)$ וב-$g_{n+p}(x)$ יהיו שקולים מודולו $\mathfrak{p}^n$; אם ניקח את הגבול $g(x) = \lim_{n\to\infty} g_n(x)$ (כל מקדם בנפרד), מהשלמות של $\mathcal{O}$ נקבל ש-$g(x) \in \mathcal{O}[x]$ (ובדומה $h(x) = \lim_{n\to\infty} h_n(x) \in \mathcal{O}[x]$).
נטען שאלו הפולינומים הנכונים. אכן, הרדוקציות של $g(x)$ ו-$h(x)$ הן $\overline{g}(x)$ ו-$\overline{h}(x)$, ומתקיים $\deg g(x) = \deg \overline{g}(x)$ אוטומטית. נותר להוכיח כי $f(x) = g(x) \cdot h(x)$. לכל n, מתקיים

$$f(x) \equiv g_n(x) h_n(x) \pmod{\mathfrak{p}^{n+1}}.$$

אבל גם

$$g(x) h(x) \equiv g_n(x) h_n(x) \pmod{\mathfrak{p}^{n+1}},$$

לכן

$$f(x) \equiv g(x) h(x) \pmod{\mathfrak{p}^{n+1}}.$$

מהשלמות נובע ש-$\bigcap_{n=1}^{\infty} \mathfrak{p}^n = 0$, ולכן $f(x) = g(x) h(x)$, כנדרש.
כעת נבנה את הסדרות. נניח שבנינו את $g_{n-1}(x)$ ואת $h_{n-1}(x)$. אפשר לרשום

$$f(x) - g_{n-1}(x) h_{n-1}(x) = \sum_{i \in I} a_i \varphi_i(x)$$

עבור $a_i \in \mathfrak{p}^n$ ו-$\varphi_i(x) \in \mathcal{O}[x]$. כיוון ש-$\overline{g}(x)$ ו-$\overline{h}(x)$ זרים, אפשר לכתוב

$$\overline{\varphi_i}(x) = c_i(x)\,\overline{g}(x) + d_i(x)\,\overline{h}(x)$$

כאשר $c_i(x), d_i(x) \in k[x]$. אבל $k[x]$ תחום אוקלידי, לכן אפשר לחלק

$$d_i(x) = q(x)\,\overline{g}(x) + \overline{r_i}(x)$$

כאשר $q(x), \overline{r_i}(x) \in k[x]$, $\deg \overline{r_i}(x) < \deg \overline{g}(x)$. אזי

$$\overline{\varphi_i}(x) = \underbrace{\left(c_i(x) + q(x)\,\overline{h}(x)\right)}_{\overline{s_i}(x)}\overline{g}(x) + \overline{r_i}(x)\,\overline{h}(x).$$

תהיינה $r_i(x), s_i(x) \in \mathcal{O}[x]$ הרמות של $\overline{r_i}(x), \overline{s_i}(x)$ עם $\deg r_i(x) = \deg \overline{r_i}(x)$. נגדיר

$$g_n(x) = g_{n-1}(x) + \sum_{i \in I} a_i \cdot r_i(x),$$
$$h_n(x) = h_{n-1}(x) + \sum_{i \in I} a_i \cdot s_i(x).$$

אז מתקיים

$$\begin{aligned} f(x) - g_n(x)\,h_n(x) &= f(x) - g_{n-1}(x)\,h_{n-1}(x) - \\ &- \sum_{i \in I} a_i\left(g_{n-1}(x)\,s_i(x) + h_{n-1}(x)\,r_i(x)\right) + \sum_{i \in I} \underbrace{a_i^2}_{\in \mathfrak{p}^{2n}} r_i(x)\,s_i(x) \equiv \\ &\equiv \sum_{i \in I} a_i\left(\varphi_i(x) - g_{n-1}(x)\,s_i(x) - h_{n-1}(x)\,r_i(x)\right) \pmod{\mathfrak{p}^{n+1}} \end{aligned}$$

אם נסתכל על הרדוקציה של הגורם בסוגריים ל-$k[x]$, נקבל

$$\overline{\varphi_i}(x) - \overline{g}(x)\,\overline{s_i}(x) - \overline{h}(x)\,\overline{r_i}(x) = 0.$$

בשילוב עם העובדה ש-$a_i \in \mathfrak{p}^n$, נקבל

$$f(x) - g_n(x)\,h_n(x) \equiv 0 \pmod{\mathfrak{p}^{n+1}}.$$

□

כעת נראה כמה יישומים של למת הנזל.

מסקנה 4.31. יהי K שדה שלם ביחס להערכה לא ארכימדית $|\cdot|$, ויהי

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$$

פולינום אי-פריק. אזי

$$\max\{|a_0|, |a_1|, \ldots, |a_n|\} = \max\{|a_0|, |a_n|\}.$$

הוכחה. יהי $|a_i| = \max\{|a_0|, |a_1|, \dots, |a_n|\}$. אם נחליף את $f(x)$ ב-$\frac{f(x)}{a_i}$, נוכל להניח בלי הגבלת הכלליות כי $f(x) \in \mathcal{O}[x]$ וכי יש מקדמים הפיכים.

יהי $j = \min\{i = 0, \dots, n : |a_i| = 1\}$. לכן

$$\overline{f}(x) = x^j \cdot \left(\overline{a_n} x^{n-j} + \cdots + \underbrace{\overline{a_j}}_{\neq 0}\right)$$

פירוק לגורמים זרים של $\overline{f}(x)$. ב-$\mathcal{O}$ מתקיימת הלמה של הנזל, לכן $f(x) = g(x) h(x)$ כאשר $\deg g(x) = j$. אבל f אי-פריק, לכן יש שתי אפשרויות: $g(x)$ קבוע ואז $j = 0$, או ש-$h(x)$ קבוע ואז $j = n$. לכן a_0 או a_n מגיעים להערכה המקסימלית. □

כדוגמה, נחזור ל-$\mathbb{Q}_p$. חוג השלמים שלו הוא $\mathcal{O} = \mathbb{Z}_p$.

טענה 4.32. $\mathbb{Z}_p$ הוא הסגור של $\mathbb{Z}$ ב-$\mathbb{Q}_p$. במילים אחרות: יהי $x \in \mathbb{Q}_p$. אזי $x \in \mathbb{Z}_p$ אם ורק אם יש סדרת קושי $\{a_n\}_{n=1}^{\infty}$ של מספרים שלמים שמציגה את המחלקה x.

הוכחה. $\boxed{\Rightarrow}$ תהי $\{a_n\}_{n=1}^{\infty}$ סדרת קושי של שלמים. אזי $|a_n|_p \leq 1$ לכל n. אם $\{a_n\}$ אפסה, סיימנו, כי $0 \in \mathbb{Z}_p$; אחרת, $\left\{|a_n|_p\right\}$ מתייצבת, ולכן $|x|_p = |a_n|_p \leq 1$ (עבור n מספיק גדול), כלומר $x \in \mathbb{Z}_p$.

$\boxed{\Leftarrow}$ יהי $x \in \mathbb{Z}_p$. אם $x = 0$, ניקח את $(0, 0, \dots)$ כסדרת קושי במחלקה של x. לכן נניח $x \neq 0$, כלומר $0 < |x|_p \leq 1$. תהי $\{a_n\}_{n=1}^{\infty}$ סדרת קושי שמציגה את x. כפי שראינו, $\left\{|a_n|_p\right\}$ מתייצבת. נוכל להשליך מספר סופי של איברים ולהניח $|x|_p = |a_n|_p \leq 1$ לכל n.

נכתוב $a_n = \frac{\alpha_n}{\beta_n}$ כשבר מצומצם. $|a_n|_p \leq 1$, לכן $p \nmid \beta_n$ לכל n. יהי y_n הפתרון למשוואה

$$\beta_n y_n \equiv \alpha_n \pmod{p^n}.$$

לכן $\beta_n y_n = \alpha_n + \gamma_n p^n$ עבור $\gamma_n \in \mathbb{Z}$. מכאן

$$y_n = a_n + \frac{\gamma_n}{\beta_n} p^n \Longrightarrow |y_n - a_n|_p = \underbrace{\left|\frac{\gamma_n}{\beta_n}\right|_p}_{\leq 1} \cdot |p^n|_p \leq \frac{1}{p^n}.$$

הראינו שהסדרה $y_n - a_n$ אפסה, ומכאן ש-y_n גם היא מציגה את x. אך זו סדרה של מספרים שלמים, כמבוקש. □

טענה 4.33. לכל n מתקיים

$$\mathbb{Z}_p/\mathfrak{p}^n = \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

בפרט, שדה השאריות של $\mathbb{Z}_p$ הוא $k \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

הוכחה. יהי $x \in \mathbb{Z}_p$, ותהי $\{a_n\}_{n=1}^{\infty}$ סדרת קושי של מספרים שלמים שמציגה את x. נשליך מספר סופי של איברים מהסדרה כך שלכל i, j יתקיים

$$|a_i - a_j|_p \leq \frac{1}{p^n}.$$

לכן

$$,a_i \equiv a_j \pmod{p^n}$$

כלומר מודולו p^n הסדרה $\{a_n\}$ קבועה. □

טענה 4.34. בחוג $\mathbb{Z}_p$ יש $p-1$ שורשים $(p-1)$-ים של 1.

הוכחה. ניקח $f(x) = x^{p-1} - 1$. כעת,

$$.\overline{f}(x) = \prod_{\lambda \in \mathbb{F}_p^\times} (x - \lambda)$$

לפי למת הנזל ואינדוקציה, $f(x)$ מתפרק לגורמים לינאריים ב-$\mathbb{Z}_p[x]$, כנדרש. □

משפט 4.35 (משפט הקירוב). יהי K שדה, ותהיינה $|\cdot|_1, \ldots, |\cdot|_n$ הערכות לא-טריוויאליות שאינן שקולות זו לזו. יהיו $a_1, \ldots, a_n \in K$. אזי לכל $\varepsilon > 0$ קיים $x \in K$ כך ש-$|x - a_i|_i < \varepsilon$ לכל $1 \leq i \leq n$.

הוכחה. נעבוד במספר שלבים.

צעד 1. תהי $|\cdot|$ הערכה על K, ויהי $z \in K$. אזי

$$\frac{z^m}{1+z^m} \to \begin{cases} 0, & |z| < 1 \\ 1, & |z| > 1 \end{cases}$$

צעד 2. נראה שקיימים $x, y \in K$ שעבורם $\begin{cases} |x|_1 < 1 \\ |x|_n > 1 \end{cases}$ ו-$\begin{cases} |y|_1 > 1 \\ |y|_n < 1 \end{cases}$.

ראשית, מספיק למצוא אחד מהם, ואז ניקח $y = x^{-1}$ (או להיפך). כאשר הוכחנו ששתי הערכות שקולות אם ורק אם $|x|_1 = |x|_n^s$, הראינו כי שתי הערכות שקולות אם ורק אם

$$.\{x \in K : |x|_1 < 1\} \subseteq \{x \in K : |x|_n < 1\}$$

לפי ההנחה שלנו, $|\cdot|_1$ ו-$|\cdot|_n$ אינן שקולות; לכן קיימים $\alpha, \beta \in K^\times$ שעבורם

$$.\begin{cases} |\alpha|_1 < 1 \\ |\alpha|_n \geq 1 \end{cases}, \qquad \begin{cases} |\beta|_1 \geq 1 \\ |\beta|_n < 1 \end{cases}$$

אז אפשר לקחת $x = \frac{\alpha}{\beta}$ ו-$y = \frac{\beta}{\alpha}$.

צעד 3. קיים $z \in K$ כך ש-$|z|_1 > 1$ ו-$|z|_i < 1$ לכל $2 \leq i \leq n$.

נוכיח זאת באינדוקציה, כאשר המקרה $n = 2$ הוא צעד 2.

נניח שהטענה נכונה עבור $n - 1$. זה אומר שקיים $z \in K$ כך ש-$|z|_1 > 1$ ו-$|z|_i < 1$ לכל $2 \leq i \leq n-1$. נחלק לשלושה מקרים:

- אם $|z|_n < 1$, סיימנו.
- אם $|z|_n = 1$, נחליף את z ב-yz^m עבור חזקה m גדולה מספיק.
- אם $|z|_n > 1$, נחליף את z ב-$\frac{yz^m}{1+z^m}$ עבור חזקה m גדולה מספיק.

צעד 4. יהי $M = \max\left\{|a_i|_j : 1 \le i, j \le n\right\}$. לפי צעד 3, קיימים $z_1, \ldots, z_n \in K$ שעבורם

$$\forall j \neq i : |z_i|_j < 1 \qquad , |z_i|_i > 1 \,.$$

לפי צעד 1, $\frac{z_i^m}{1+z_i^m} \to 1$ לפי $|\cdot|_i$ ו-$\frac{z_i^m}{1+z_i^m} \to 0$ לפי שאר ההערכות. אם כן, ניקח

$$w_i = \frac{z_i^m}{1+z_i^m}$$

עבור m מספיק גדול כך שיתקיים

$$\forall j \neq i : |w_i|_j < \frac{\varepsilon}{Mn} \qquad , |w_i - 1|_i < \frac{\varepsilon}{Mn} \,.$$

יהי $x = a_1 w_1 + \cdots + a_n w_n$. לכל i מתקיים

$$\begin{aligned} |x - a_i|_i &= |a_1 w_1 + \cdots + a_i (w_i - 1) + \cdots + a_n w_n|_i \le \\ &\le |a_1|_i |w_1|_i + \cdots + |a_i|_i |w_i - 1|_i + \cdots + |a_n|_i |w_n|_i < \\ &< M \cdot \frac{\varepsilon}{Mn} \cdot n = \varepsilon \end{aligned}$$

כנדרש.

□

הערה. אפשר לחשוב על משפט הקירוב כהכללה של משפט השאריות הסיני, כאשר לוקחים את ההערכות להיות ההערכות ה-p-אדיות.

משפט 4.36 (אוסטרובסקי)**.** יהי K שדה שלם ביחס להערכה ארכימדית. אזי $K \cong \mathbb{R}$ או $K \cong \mathbb{C}$, וההערכה שקולה להערכה הרגילה.

4.4 הערכות והרחבות שדות

משפט 4.37. יהי K שדה שלם ביחס להערכה $|\cdot|$, ותהי L/K הרחבה אלגברית. אזי יש דרך יחידה להמשיך את $|\cdot|$ להערכה על L. יתרה מזאת, L עדיין שלם תחת ההערכה הזו.
אם L/K סופית מדרגה n, אזי לכל $\alpha \in L$ מתקיים

$$|\alpha| = \sqrt[n]{\left|\mathrm{N}_{L/K}(\alpha)\right|} \,.$$

הוכחה. ראשית, מספיק להוכיח את המשפט עבור הרחבות סופיות; הרחבה אלגברית היא איחוד של הרחבות סופיות, ובגלל היחידות אפשר "להדביק" הערכות. לכן נניח ש-L/K סופית מדרגה n. לפי משפט אוסטרובסקי, ניתן להניח כי $|\cdot|$ לא ארכימדית.

קיום. יהי $\mathcal{O}_K = \{x \in K : |x| \le 1\}$ חוג השלמים של K, ויהי $\mathcal{O}_L$ הסגור השלם של $\mathcal{O}_K$ ב-L. יהי $\alpha \in L$, ויהי $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ הפולינום המינימלי של α.
באופן כללי, $\mathrm{N}_{L/K}(\alpha) = \pm a_0^m$; אם $\alpha \in \mathcal{O}_L$, מהטענות הכלליות מתחילת הקורס נקבל כי $\mathrm{N}_{L/K}(\alpha) \in \mathcal{O}_K$.
מצד שני, נניח כי $\mathrm{N}_{L/K}(\alpha) \in \mathcal{O}_K$. מכאן $|\pm a_0|^m \le 1$, כלומר $|a_0| \le 1$. הפולינום $f(x)$ אי-פריק, ולכן ממסקנה 4.31 נקבל כי

$$\max\{|a_0|, |a_1|, \ldots, |a_d|\} = \max\{|a_0|, |a_d|\} = 1 \,.$$

זה אומר ש-$f(x) \in \mathcal{O}_K[x]$, כלומר α שלם מעל $\mathcal{O}_K$, ולכן $\alpha \in \mathcal{O}_L$.
אם כן, הוכחנו כי $\alpha \in \mathcal{O}_L$ אם ורק אם $\mathrm{N}_{L/K}(\alpha) \in \mathcal{O}_K$. אם נגדיר $\|\alpha\| = \sqrt[n]{\left|\mathrm{N}_{L/K}(\alpha)\right|}$ לכל $\alpha \in L$, בעצם הוכחנו כי $\alpha \in \mathcal{O}_L$ אם ורק אם $\|\alpha\| \le 1$.
נרצה להוכיח כי $\|\cdot\|$ הערכה על L. האקסיומה היחידה שאינה ברורה היא אי-שוויון המשולש. כיוון ש-$\mathcal{O}_L$ הוא חוג,

$$\alpha \in \mathcal{O}_L \iff \alpha + 1 \in \mathcal{O}_L.$$

לפי מה שהוכחנו קודם,

$$\|\alpha\| \le 1 \iff \|\alpha + 1\| \le 1\,.$$

יהיו $x, y \in L$ כך ש-$\|x\| \le \|y\|$. ניתן להניח כי $y \neq 0$, ואז $\left\|\frac{x}{y}\right\| \le 1$. מכאן

$$\left\|\frac{x}{y} + 1\right\| \le 1 \Longrightarrow \|x + y\| \le \|y\| = \max\{\|x\|, \|y\|\}\,.$$

קיבלנו את אי-שוויון המשולש החזק, לכן $\|\cdot\|$ אכן הערכה על L.

יחידות. תהי $|\alpha| = \sqrt[n]{\left|\mathrm{N}_{L/K}(\alpha)\right|}$, ויהי $\mathcal{O}_L$ חוג השלמים שלה. תהי $|\cdot|'$ הערכה אחרת על L שממשיכה את ההערכה הנתונה על K, ויהי $\mathcal{O}'$ חוג השלמים שלה. נרצה להוכיח כי $|\cdot|' = |\cdot|$.
יהי $\alpha \in \mathcal{O}_L$. הפולינום המינימלי של α מעל K הינו $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ עבור $a_0, \ldots, a_{d-1} \in \mathcal{O}_K$. נניח בשלילה כי $|\alpha|' > 1$. יהי $\mathfrak{p}'$ האידאל המקסימלי של $\mathcal{O}'$; לכן $\frac{1}{\alpha} \in \mathfrak{p}'$. מצד שני,

$$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$$

ולכן

$$1 = -a_{d-1} \cdot \frac{1}{\alpha} - \cdots - a_0 \cdot \left(\frac{1}{\alpha}\right)^d.$$

כיוון ש-$\mathcal{O}_K \subseteq \mathcal{O}'$, זה מוכיח ש-$1 \in \mathfrak{p}'$, בסתירה.
מהסתירה נסיק כי $\mathcal{O}_L \subseteq \mathcal{O}'$. כפי שעשינו במשפט הקירוב, זה מראה ש-$|\cdot|$ ו-$|\cdot|'$ שקולות זו לזו. זה אומר שקיים $s > 0$ שעבורו $|\alpha|' = |\alpha|^s$ לכל $\alpha \in L$. אם ניקח $\alpha \in K$ כך ש-$|\alpha| \neq 0, 1$ (קיים כזה כי $|\cdot|$ אינה טריוויאלית), נקבל כי $s = 1$. לכן $|\cdot|' = |\cdot|$.

שלמות. זה ינבע מהטענה הבאה:

טענה 4.38. יהי K שדה שלם ביחס להערכה לא ארכימדית $|\cdot|$. יהי V מרחב וקטורי סוף-מימדי מעל K, ותהי $\|\cdot\|$ נורמה על V, כלומר פונקציה המקיימת:

- $\|v\| = 0 \iff v = 0$.
- $\|\alpha v\| = |\alpha|\,\|v\|$.
- $\|v + w\| \le \|v\| + \|w\|$.

נבחר בסיס $v_1,\dots,v_n$ של V, ונגדיר נורמה

$$\|\alpha_1 v_1+\cdots+\alpha_n v_n\|_{\max}=\max\{|\alpha_1|,\dots,|\alpha_n|\}.$$

אזי הנורמות $\|\cdot\|$ ו-$\|\cdot\|_{\max}$ שקולות (כלומר מגדירות את אותה הטופולוגיה המטרית).

נראה כיצד הטענה מוכיחה את השלמות של L. נבחר בסיס $v_1,\dots,v_n$ של L מעל K, ונטען ש-L שלם ביחס לנורמה $\|\cdot\|_{\max}$.

אכן, תהי $\{\beta_m\}_{m=1}^{\infty}$ סדרת קושי לפי $\|\cdot\|_{\max}$. נכתוב $\beta_m=\alpha_1^{(m)}v_1+\cdots+\alpha_n^{(m)}v_n$. לפי הגדרת $\|\cdot\|_{\max}$, כל הסדרות $\left\{\alpha_i^{(m)}\right\}_{m=1}^{\infty}$ הן סדרות קושי ב-K; אך K שלם, לכן יש להן גבולות $\ell_i\in K$. כעת נגדיר $w=\ell_1 v_1+\cdots+\ell_n v_n$, ונקבל ש-$\beta_m\to w$. לכן L שלם ביחס ל-$\|\cdot\|_{\max}$.

מהטענה קיבלנו כי $|\cdot|$ שקולה ל-$\|\cdot\|_{\max}$, ושלמות היא תכונה טופולוגית; לכן L שלם ביחס ל-$|\cdot|$. □

הוכחת טענה 4.38. מספיק להוכיח כי קיימים קבועים $C,C'>0$ המקיימים

$$C\cdot\|v\|_{\max}\le\|v\|\le C'\cdot\|v\|_{\max}$$

לכל $v\in V$. נרשום $v=\alpha_1 v_1+\cdots+\alpha_n v_n$; מתקיים

$$\begin{aligned}\|v\|&\le\|\alpha_1 v_1\|+\cdots+\|\alpha_n v_n\|=|\alpha_1|\,\|v_1\|+\cdots+|\alpha_n|\,\|v_n\|\le\\&\le\underbrace{\max\{|\alpha_1|,\dots,|\alpha|_n\}}_{\|v\|_{\max}}\cdot\underbrace{(\|v_1\|+\cdots+\|v_n\|)}_{C'}=C'\cdot\|v\|_{\max}\end{aligned}$$

בשביל להוכיח שקיים C כנ"ל, נשתמש באינדוקציה על $\dim V$. נניח $\dim V=1$, ויהי $0\ne v_1\in V$. אזי

$$\|v\|=\|\alpha_1 v_1\|=|\alpha_1|\cdot\|v_1\|=\|v\|_{\max}\cdot\|v_1\|$$

ואפשר לקחת $C=\|v_1\|$ ולקבל שוויון.

כעת נניח שהטענה ידועה עבור מימד $n-1$. ניקח

$$V_i=\operatorname{Span}\{v_1,\dots,v_{i-1},v_{i+1},\dots,v_n\}.$$

לפי הנחת האינדוקציה, כל V_i שלם תחת הצמצום של $\|\cdot\|$ אליו. בפרט, כל V_i סגור בטופולוגיה המטרית של V תחת $\|\cdot\|$. לכן כל ההזזות V_i+v_i סגורות, ומכאן שגם $\bigcup_{i=1}^{n}(V_i+v_i)$ סגורה.

אבל $0\notin\bigcup_{i=1}^{n}(V_i+v_i)$; לכן קיימת סביבה פתוחה $0\in U\subseteq V$ שמוכלת במשלים של $\bigcup_{i=1}^{n}(V_i+v_i)$. בפרט, קיים $C>0$ כך ש-$\{v\in V:\|v\|<C\}\subseteq U$. זה אומר שלכל $v\in\bigcup_{i=1}^{n}(V_i+v_i)$, $\|v\|\ge C$.

יהי $v=\alpha_1 v_1+\cdots+\alpha_n v_n\in V$, ויהי $|\alpha_i|=\|v\|_{\max}$. ניתן להניח ש-$v\ne 0$, ואז

$$\frac{1}{\alpha_i}v=\frac{\alpha_1}{\alpha_i}v_1+\cdots+v_i+\cdots+\frac{\alpha_n}{\alpha_i}v_n\in\bigcup_{i=1}^{n}(V_i+v_i).$$

לכן

$$\left\|\frac{1}{\alpha_i}v\right\|\ge C\Longrightarrow\|v\|\ge C\cdot|\alpha_i|=C\cdot\|v\|_{\max},$$

וסיימנו. □

4.5 הערכות אקספוננציאליות

טענה 4.39. תהי $|\cdot|$ הערכה לא ארכימדית על שדה K. נתבונן בפונקציה $v:K\to\mathbb{R}\cup\{\infty\}$ המוגדרת לפי

$$v(\alpha)=-C\cdot\log|\alpha|$$

עבור $C>0$. אזי v מקיימת את התכונות הבאות:

א. $v(\alpha)=\infty\iff\alpha=0$.

ב. $v(\alpha\beta)=v(\alpha)+v(\beta)$ לכל $\alpha,\beta\in K$.

ג. $v(\alpha+\beta)\geq\min\{v(\alpha),v(\beta)\}$ לכל $\alpha,\beta\in K$.

הגדרה 4.40. פונקציה $v:K\to\mathbb{R}\cup\{\infty\}$ המקיימת את התנאים הנ"ל נקראת **הערכה אקספוננציאלית** על K.

אמנם זה מושג שקול למושג של הערכה כפלית שהגדרנו, אך לפעמים השימוש בו מייצר שפה נוחה יותר.

דוגמה 4.41. נסתכל על $|\cdot|_p$ על $K=\mathbb{Q}$, וניקח $C=\frac{1}{\log p}$. אם $\alpha=p^c\cdot\frac{m}{n}$ עבור $p\nmid m,n$, אז

$$|\alpha|_p=\frac{1}{p^c}\Longrightarrow v(\alpha)=-\log_p|\alpha|_p=c\ .$$

כלומר $v(\alpha)=c$ אם ורק אם $\alpha\mathbb{Z}=(p\mathbb{Z})^c\cdot I$, כאשר I אידאל שברי שזר ל-$p\mathbb{Z}$.

כעת אפשר לתרגם כל משפט שהיה לנו לשפה של הערכות אקספוננציאליות. למשל, נתרגם את טענה 4.8:

טענה 4.42. אם $v(\alpha)\neq v(\beta)$, אז $v(\alpha+\beta)=\min\{v(\alpha),v(\beta)\}$.

דוגמה 4.43. יהי K שדה מספרים, יהי $\mathcal{O}_K$ שדה השלמים (במובן הרגיל) של K, ויהי $\mathfrak{p}\subseteq\mathcal{O}_K$ אידאל ראשוני. אפשר להגדיר הערכה $\mathfrak{p}$-אדית על K באופן הבא: יהי $\alpha\in K^\times$. נכתוב $\alpha\mathcal{O}_K=\mathfrak{p}^c\cdot I$ כאשר I אידאל שברי שזר ל-$\mathfrak{p}$. נגדיר

$$v_\mathfrak{p}(\alpha)=c\,,\ |\alpha|_\mathfrak{p}=\left(\frac{1}{\mathrm{N}(\mathfrak{p})}\right)^c\ .$$

אפשר לבנות את ההשלמה $\widehat{K}=K_\mathfrak{p}$ (ביחס ל-$|\cdot|_\mathfrak{p}$). $\mathbb{Q}_p\subseteq K_\mathfrak{p}$ אם ורק אם $p\mid\mathfrak{p}$.

מעתה והלאה, v תמיד תסמן הערכה אקספוננציאלית.

הגדרה 4.44. יהי K שדה עם הערכה v, ויהי $f(x)=a_nx^n+\cdots+a_1x+a_0\in K[x]$ פולינום. נתבונן בקבוצת הנקודות $\{(i,v(a_i)):0\leq i\leq n\}$. הקמור התחתון של הקבוצה הזו נקרא **מצולע ניוטון** של $f(x)$.

טענה 4.45. יהי L/K שדה הפיצול של $f(x)$, תהי v הערכה על K, ותהי w הערכה על L שממשיכה את ההערכה v. נשים לב שמצולע ניוטון הוא איחוד של קטעים. אם אחד הקטעים הוא הקטע מ-$(r,v(a_r))$ ל-$(s,v(a_s))$, אזי ל-$f(x)$ יש $s-r$ שורשים בעלי הערכה w ששווה

$$-\frac{v(a_s)-v(a_r)}{s-r}$$

(שהוא גם הנגדי של שיפוע הקטע).

הוכחה. יהיו $\alpha_1,\ldots,\alpha_n \in L$ השורשים של $f(x)$ ב-L. נמספר אותם כך שיתקיים

$$\begin{aligned} w(\alpha_1)=\cdots=w(\alpha_{s_1}) &= m_1 \\ w(\alpha_{s_1+1})=\cdots=w(\alpha_{s_2}) &= m_2 \\ &\vdots \\ w\left(\alpha_{s_{t-1}+1}\right)=\cdots=w(\alpha_n) &= m_t \end{aligned}$$

כאשר $m_1<m_2<\cdots<m_t$. מתקיים

$$f(x)=a_nx^n+\cdots+a_1x+a_0=a_n\cdot\prod_{i=1}^{n}(x-\alpha_i).$$

בלי הגבלת הכלליות, נניח כי $a_n=1$. מותר לעשות את זה כי זה לא משפיע על השורשים ולא על השיפוע (נקבל הזזה של מצולע ניוטון). בפרט $v(a_n)=0$. לכן

$$\begin{aligned} a_{n-1}=\pm(\alpha_1+\cdots+\alpha_n) &\Longrightarrow v(a_{n-1})=w(a_{n-1})\geq\min\{w(\alpha_i)\}=m_1 \\ a_{n-2}=\pm\left(\sum_{i\neq j}\alpha_i\alpha_j\right) &\Longrightarrow v(a_{n-2})\geq\min\{w(\alpha_i\alpha_j)\}=2m_1 \\ &\vdots \end{aligned}$$

כך אפשר להמשיך עד שמגיעים למקדם ה-s_1:

$$v(a_{n-s_1})=w\left(\sum\alpha_{i_1}\ldots\alpha_{i_{s_1}}\right)=m_1s_1$$

כי הפעם יש מחובר יחיד עם הערכה מינימלית. כעת אפשר להמשיך עוד:

$$\begin{aligned} v(a_{n-s_1-1}) &\geq \min\left\{w\left(\alpha_{i_1}\ldots\alpha_{i_{s_1+1}}\right)\right\}=m_1s_1+m_2 \\ &\vdots \\ v(a_{n-s_2}) &= m_1s_1+m_2(s_2-s_1) \end{aligned}$$

וכן הלאה. אבל בעצם מה שהראינו הוא שמצולע ניוטון מוגדר על ידי הקודקודים

$$(n-s_i, m_1s_1+m_2(s_2-s_1)+\cdots+m_i(s_i-s_{i-1})),$$

וזה מוכיח את הטענה. □

יהי $f(x)$ כנ"ל, ויהיו $m_1,\ldots,m_r$ ההערכות השונות של השורשים שלו. יהיו

$$f_j(x)=\prod_{\substack{f(\alpha)=0\\ w(\alpha)=m_j}}(x-\alpha),$$

כלומר $f(x)=a_n\cdot f_1(x)\cdot\cdots\cdot f_r(x)$.

טענה 4.46. יהי L שדה הפיצול של $f(x)$. נניח ש-v ממשיכה באופן יחיד להערכה w על L. אזי $f_j(x) \in K[x]$ לכל $1 \le j \le r$.

הוכחה. בלי הגבלת הכלליות, אפשר להניח כי $f(x)$ מתוקן.

נתחיל מלהניח ש-$f(x)$ אי-פריק. אם α שורש של $f(x)$, אז כל שורש אחר של $f(x)$ הוא $\sigma(\alpha)$ לאיזשהו $\sigma \in \mathrm{Gal}\left({}^{L}\!/_{K}\right)$. אבל $w \circ \sigma$ היא גם הערכה על L שממשיכה את v; מהיחידות נקבל ש-$w(\alpha) = w \circ \sigma(\alpha)$, ולכן לכל השורשים יש אותה הערכה, כלומר $f(x) = f_1(x)$.

במקרה הכללי, נעבור לאינדוקציה על $n = \deg f(x)$. יהי α_1 שורש של $f(x)$ עם $w(\alpha_1) = m_1$, ויהי $g_1(x) \in K[x]$ הפולינום המינימלי של α_1 מעל K. לכן $f(x) = g_1(x) \cdot g(x)$, כאשר $g(x) \in K[x]$, ומתקיים

$$g(x) = \frac{f_1(x)}{g_1(x)} \cdot f_2(x) \cdot \dots \cdot f_r(x).$$

אבל $\deg g(x) < \deg f(x)$. מהנחת האינדוקציה, $\frac{f_1(x)}{g_1(x)}, f_2(x), \dots, f_r(x) \in K[x]$; לכן גם $f_1(x) = \frac{f_1(x)}{g_1(x)} \cdot g_1(x) \in K[x]$. □

מסקנה 4.47. אם $f(x)$ אי-פריק ו-v ממשיכה באופן יחיד לשדה הפיצול של $f(x)$, אזי מצולע ניוטון של $f(x)$ הינו קטע אחד. בפרט,

$$\min\{v(a_0), v(a_1), \dots, v(a_n)\} = \min\{v(a_0), v(a_n)\}.$$

ראינו זאת בעבר כמסקנה מלמת הנזל (מסקנה 4.31), וכעת אנו רואים זאת במקרה של המשכה יחידה של v ל-L.

4.6 שדות הנזליים

הגדרה 4.48. שדה K עם הערכה לא ארכימדית $|\cdot|$ נקרא **הנזלי**, אם חוג ההערכה

$$\mathcal{O}_K = \{\alpha \in K : |\alpha| \le 1\} = \{\alpha \in K : v(\alpha) \ge 0\}$$

מקיים את הלמה של הנזל.

דוגמה 4.49. ראינו כי אם K שלם ביחס להערכה בדידה, אזי K הנזלי (משפט 4.30).

טענה 4.50. יהי K שדה שלם עם הערכה לא ארכימדית. אזי K הנזלי אם ורק אם לכל הרחבה אלגברית ${}^{L}\!/_{K}$ ניתן להמשיך את v ל-L באופן יחיד.

הוכחה. $\boxed{\Leftarrow}$ ראינו במשפט 4.37 (במשפט מופיעה ההנחה ש-K שלם, אך למעשה רק השתמשנו בלמה של הנזל).

$\boxed{\Rightarrow}$ נניח שיש המשכות יחידות.

טענה. יהי $f(x) \in \mathcal{O}_K[x]$ פולינום אי-פריק ופרימיטיבי (כלומר $\overline{f}(x) \neq 0$, ובאופן שקול מתקיים $\max\{|\text{מקדמים של } f(x)|\} = 1$). אזי $\overline{f}(x) \in k[x]$ קבוע או ש-$\deg \overline{f}(x) = \deg f(x)$ ו-$\overline{f}(x) = \overline{a} \cdot \overline{\varphi}(x)^m$ כאשר $\overline{a} \in k^\times$ ו-$\overline{\varphi} \in k[x]$ אי-פריק.

הוכחה. יהי $f(x) = a_n x^n + \cdots + a_1 x + a_0$. אם $a_n \in \mathfrak{p}_K$, אזי $|a_0| = 1$, כי

$$1 = \max\{|a_0|, |a_1|, \ldots, |a_n|\} = \max\{|a_0|, |a_n|\}.$$

אם כן, מצולע ניוטון של $f(x)$, שהוא קטע אחד, הוא הקטע מ-$(0,0)$ ל-$(n, v(a_n))$. בפרט, $v(a_i) > 0$ לכל $i > 0$, כלומר $a_i \in \mathfrak{p}_K$ לכל $i > 0$, ומכאן ש-$\overline{f}(x) = \overline{a_0}$ קבוע.

לכן נניח $a_n \in \mathcal{O}_K^\times$; כלומר $\deg \overline{f}(x) = \deg f(x)$. יהי L שדה הפיצול של $f(x)$, ויהי α שורש של $f(x)$. כל שורש אחר הינו $\sigma(\alpha)$ לאיזשהו $\sigma \in \mathrm{Gal}(L/K)$. מעל L, נקבל

$$f(x) = a_n \cdot \prod_{\sigma \in \mathrm{Gal}(L/K)} (x - \sigma(\alpha)),$$

כיוון שיש המשכה יחידה w של v ל-L, לכל $\sigma \in \mathrm{Gal}(L/K)$ מתקיים $w \circ \sigma = w$. כלומר σ שומר על $\mathcal{O}_L$ ועל $\mathfrak{p}_L$, ובפרט משרה k-אוטומורפיזם של $\ell = \mathcal{O}_L/\mathfrak{p}_L$. לכן

$$\overline{f}(x) = \overline{a_n} \cdot \prod_{\sigma \in \mathrm{Gal}(L/K)} \left(x - \overline{\sigma(\alpha)}\right) = \overline{a_n} \cdot \prod_{\sigma \in \mathrm{Gal}(L/K)} (x - \overline{\sigma}(\overline{\alpha})).$$

מכאן שכל השורשים של $\overline{f}(x)$ צמודים, לכן יש ל-$\overline{f}(x)$ רק גורם ראשוני אחד ב-$k[x]$, וסיימנו. □

כעת נוכיח את הלמה של הנזל עבור $\mathcal{O}_K$. יהי $f(x) \in \mathcal{O}_K[x]$ פולינום פרימיטיבי, יהי $\overline{f}(x) = \overline{g}(x) \cdot \overline{h}(x)$ פירוק לגורמים זרים, ויהי

$$f(x) = f_1(x) \ldots f_r(x)$$

הפירוק לגורמים אי-פריקים. לכן

$$\overline{f}(x) = \overline{f_1}(x) \cdot \cdots \cdot \overline{f_r}(x)$$

כשכל $\overline{f_i}(x)$ קבוע או עם $\deg \overline{f_i}(x) = \deg f_i(x)$ ו-$\overline{f_i}(x) = \overline{a_i} \cdot \overline{\varphi_i}(x)^{m_i}$. אבל זה אומר שעד כדי סקלרים,

$$\overline{g}(x) = \overline{a} \cdot \prod_{i \in I} \overline{f_i}(x), \qquad \overline{h}(x) = \overline{b} \cdot \prod_{j \in J} \overline{f_j}(x)$$

כאשר $I \cap J = \varnothing$, $I \cup J = \{1, \ldots, r\}$, ולכל $i \in I$ מתקיים $\deg \overline{f_i}(x) = \deg f_i(x)$. ניקח

$$g(x) = a \cdot \prod_{i \in I} f_i(x), \qquad h(x) = b \cdot \prod_{j \in J} f_j(x)$$

כאשר $a, b \in \mathcal{O}_K$ הרמות מתאימות של $\overline{a}, \overline{b}$. לכן $\deg \overline{g}(x) = \deg g(x)$, כנדרש. □

דוגמה 4.51. $K = \mathbb{Q}$ עם $|\cdot|_p$ הוא לא הנזלי. נראה זאת במקרה $p \neq 2$.

אכן, נבחר d עם $d \equiv 2, 3 \pmod 4$, $p \nmid d$, $\left(\frac{d}{p}\right) = 1$ – כלומר p מתפרק לגורמים שונים ב-$L = \mathbb{Q}\left(\sqrt{d}\right)$. אז $x^2 - d = \left(x + \sqrt{d}\right)\left(x - \sqrt{d}\right)$. לכן מתקיים $p\mathcal{O}_L = P_1 \cdot P_2$, ואת ההערכה v_p אפשר להמשיך ל-w_{P_1} ול-w_{P_2}. לפי הטענה הקודמת, $\mathbb{Q}$ אינו הנזלי ביחס ל-$|\cdot|_p$.

4.7 יישומים ללמידת $\mathbb{Q}_p$

נתחיל מקצת מוטיבציה. יהי A תחום דדקינד, $K = \mathrm{Frac}A$, ויהי $\mathfrak{p} \subseteq A$ אידאל ראשוני. לכל $\alpha \in K^\times$ אפשר לכתוב $\alpha A = \mathfrak{p}^c \cdot I$, כאשר I אידאל שברי זר ל-$\mathfrak{p}$. מגדירים $v_\mathfrak{p}(\alpha) = c$.

תהי L/K הרחבה סופית, ויהי B הסגור השלם של A ב-L. אפשר לכתוב

$$\mathfrak{p}B = P_1^{e_1} \dots P_r^{e_r}$$

עבור אידאלים ראשוניים $P_1, \dots, P_r$ של B. אם $\mathfrak{p} \mid P$ אידאל ראשוני של B, אזי w_P היא הערכה על L שממשיכה את $v_\mathfrak{p}$ עד כדי שקילות.

יהיו L_P ו-$K_\mathfrak{p}$ ההשלמות.

עובדה. אם L/K גלואה, אז

$$\mathrm{Gal}\left(L_P/K_\mathfrak{p}\right) \cong G_P = \left\{\sigma \in \mathrm{Gal}\left(L/K\right) : \sigma(P) = P\right\}.$$

למשל, אם $A = \mathbb{Z}$, $K = \mathbb{Q}$ ו-$\mathfrak{p} = p\mathbb{Z}$ לאיזשהו ראשוני p; אז $K_\mathfrak{p} = \mathbb{Q}_p$.

אחת המטרות הגדולות של תורת המספרים היא לחקור את $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. באופן ישיר זה די קשה, אבל אפשר להשתמש בעובדה שמתקיים

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) = \varprojlim_{L/\mathbb{Q} \text{ finite Galois}} \mathrm{Gal}\left(L/\mathbb{Q}\right).$$

יהי p ראשוני. לכל $L/\mathbb{Q}$ כנ"ל אפשר נבחר אידאל $P_L \mid p\mathbb{Z}$ בצורה קומפטבילית, כלומר לכל $\mathbb{Q} \subseteq L \subseteq M$ מתקיים $P_M \mid P_L \mathcal{O}_M$. נקבל

$$\mathrm{Gal}\left(\overline{\mathbb{Q}_p}/\mathbb{Q}_p\right) = \varprojlim \mathrm{Gal}\left(L_{P_L}/\mathbb{Q}_p\right) \underset{\text{עובדה}}{\cong} \left\{\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) : \forall L : \sigma(P_L) = P_L\right\} \leq \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right).$$

לכן כדאי לנסות ללמוד את $\mathrm{Gal}\left(\overline{\mathbb{Q}_p}/\mathbb{Q}_p\right)$, וכך נבין איזושהי תת-חבורה של $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$.

דוגמה 4.52. $\overline{\mathbb{Q}_p}$, הסגור האלגברי של $\mathbb{Q}_p$, הנזלי (לפי הטענה, זה נכון באופן ריק). נטען כי $\overline{\mathbb{Q}_p}$ אינו שלם.

אכן, המימד של ההרחבה $\overline{\mathbb{Q}}/\mathbb{Q}$ הוא $\aleph_0$ (כי $\mathbb{Q}$ בת-מנייה; לכן יש מספר בן-מנייה של פולינומים מעל $\mathbb{Q}$, ולכל אחד מהם מספר סופי של שורשים). מתקיים כי $\mathrm{Gal}\left(\overline{\mathbb{Q}_p}/\mathbb{Q}_p\right) \leq \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, בפרט $\left[\overline{\mathbb{Q}_p} : \mathbb{Q}_p\right] = \aleph_0$.

יהי $v_1, v_2, \dots$ בסיס, ונניח בשלילה כי $\overline{\mathbb{Q}_p}$ שלם. נתבונן בקבוצה

$$S_i = \overline{\mathbb{Q}_p} \setminus \mathrm{Span}_{\mathbb{Q}_p}\left\{v_1, \dots, v_i\right\}.$$

לפי טענה 4.38, תת-המרחב $\mathrm{Span}_{\mathbb{Q}_p}\left\{v_1, \dots, v_i\right\}$ שלם כמרחב מטרי, כי $\mathbb{Q}_p$ שלם. לכן כל S_i פתוחה. ברור שהיא צפופה ב-$\overline{\mathbb{Q}_p}$. לפי משפט הקטגוריה של Baire, גם החיתוך $\bigcap_{i=1}^\infty S_i$ צפוף; אבל $\bigcap_{i=1}^\infty S_i = \varnothing$, בסתירה.

טענה 4.53. יהי K שדה סגור אלגברית עם הערכה לא ארכימדית, ותהי $\widehat{K}$ ההשלמה שלו. אזי השדה $\widehat{K}$ סגור אלגברית.

הוכחה. תהי $L/\widehat{K}$ הרחבה אלגברית, ויהי $\alpha \in L$. נרצה להוכיח כי $\alpha \in \widehat{K}$. כיוון ש-$\widehat{K}$ שלם, יש לנו הערכה קנונית על L. אם נכפול את α באיבר מתאים של K, נוכל להניח בלי הגבלת הכלליות כי $|\alpha| \leq 1$. יהי $f(x) \in \widehat{K}[x]$ הפולינום המינימלי של α.

לכל פולינום $g(x) = a_n x^n + \cdots + a_1 x + a_0 \in \widehat{K}[x]$ נגדיר

$|g(x)| = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$.

K צפוף ב-$\widehat{K}$, לכן יש סדרה של פולינומים $f_n(x) \in K[x]$, $\deg f_n(x) = r = \deg f(x)$, כך ש-$|f(x) - f_n(x)| < \frac{1}{2^n}$. כל $f_n(x)$ מתפרק לגורמים לינאריים, כי K סגור אלגברית. לכן

$$= |\text{האיבר החופשי של } f_n(x+\alpha)| = |\text{שורשים של } f_n(x+\alpha)| = \prod |\beta - \alpha| \prod_{\beta : f_n(\beta)=0}$$

$$= |f_n(\alpha)| = |f_n(\alpha) - f(\alpha)| = |a_r \alpha^r + \cdots + a_1 \alpha + a_0| \leq$$

$$\leq \max\{|a_r \alpha^r|, \ldots, |a_1 \alpha|, |a_0|\} < \frac{1}{2^n}$$

כשאי-השוויון האחרון נובע מכך ש-$|\alpha| \leq 1$ ו-$|f(x) - f_n(x)| < \frac{1}{2^n}$.

לכן לכל n קיים שורש β_n של $f_n(x) \in K[x]$ כך ש-$|\beta_n - \alpha| < \sqrt[r]{\frac{1}{2^n}}$, ובפרט $\beta_n \to \alpha$. אבל $\beta_n \in K$, כי K סגור אלגברית; לכן $\alpha \in \widehat{K}$, כנדרש. $\square$

מסקנה 4.54. השדה $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ סגור אלגברית ושלם.

4.8 הסתעפות בהרחבות של שדה הנזלי

הגדרה 4.55. יהי K שדה הנזלי ביחס להערכה v. תהי L/K הרחבה ממעלה n, ותהי w ההערכה (היחידה) של L שמרחיבה את v. יהיו k ו-ℓ שדות השאריות של K ו-L בהתאמה. נגדיר

$$f(w/v) = [\ell : k] \qquad , \left[w\left(L^\times\right) : v\left(K^\times\right)\right] = e(w/v).$$

הערה. מעתה והלאה, תמיד נניח ש-ℓ/k ספרבילית. נשים לב שתמיד $[\ell : k] \leq [L : K] < \infty$.

הערה 4.56. אם v בדידה, אזי $\mathcal{O}_K$ הינו **חוג הערכה בדידה** (**discrete valuation ring**), כלומר תחום ראשי מקומי. בפרט, $\mathcal{O}_K$ הוא תחום דדקינד. יהי $\mathfrak{p}_K \subseteq \mathcal{O}_K$ האידאל הראשוני היחיד של $\mathcal{O}_K$, ויהי $\mathfrak{p}_L \subseteq \mathcal{O}_L$ האידאל הראשוני היחיד של $\mathcal{O}_L$. מהנוסחה היסודית שהוכחנו,

$$n = \sum_{P_i | \mathfrak{p}_K} e(P_i/\mathfrak{p}_K) \cdot f(P_i/\mathfrak{p}_K) = e(\mathfrak{p}_L/\mathfrak{p}_K) \cdot f(\mathfrak{p}_L/\mathfrak{p}_K) = e \cdot f ,$$

כי $\mathfrak{p}_K \mathcal{O}_L = \mathfrak{p}_L^e$.

טענה 4.57. יהיו K, L כנ"ל. אזי $n = [L : K] \geq ef$. אם בנוסף v בדידה, יש שוויון.

הוכחה. את המקרה הבדיד ראינו. לכן נוכיח את אי-השוויון במקרה הכללי.
תהי $\omega_1, \ldots, \omega_f \in \mathcal{O}_L^\times$ קבוצת הרמות של בסיס של ℓ כמרחב וקטורי מעל k. בנוסף, תהי $\{\pi_i\}_{i \in I} \subseteq \mathcal{O}_L$ קבוצה כך ש-$w(\pi_i)$ נציגים של כל הקוסטים של $w(L^\times)/v(K^\times)$ (אם v בדידה, אפשר לקחת $1, \pi_L, \ldots, \pi_L^{e-1}$). נרצה להוכיח כי האיברים $\pi_i \omega_j$ בלתי-תלויים לינארית מעל K.

נניח בשלילה שלא. אז קיימים $a_{i,j} \in K$, לא כולם 0, שעבורם

$$\sum_{i,j} a_{i,j}\pi_i\omega_j = 0 .$$

לכל i נגדיר $s_i = \sum_{j=1}^{f} a_{i,j}\omega_j$. כיוון שהצירוף הלינארי הנ"ל סופי, יש מספר סופי של $s_i \neq 0$, ומתקיים $\sum_i s_i\pi_i = 0$. לכן מתקיים

$$w\left(\sum_i s_i\pi_i\right) > \min\left\{w\left(s_i\pi_i\right) : s_i \neq 0\right\}.$$

לפי טענה 4.42, זה קורה רק כאשר יש שני מחוברים שונים עם אותה הערכה מינימלית, כלומר

$$w\left(s_{i_1}\pi_{i_1}\right) = w\left(s_{i_2}\pi_{i_2}\right)$$

והם עם הערכה מינימלית. נפתח ונקבל

$$w\left(s_{i_1}\right) + w\left(\pi_{i_1}\right) = w\left(s_{i_2}\right) + w\left(\pi_{i_2}\right) \Longrightarrow w\left(\pi_{i_1}\right) - w\left(\pi_{i_2}\right) = w\left(s_{i_2}\right) - w\left(s_{i_1}\right).$$

אם נוכיח שלכל i, $w\left(s_i\right) \in v\left(K^\times\right)$, נקבל סתירה לכך שה-$\pi_i$-ים הם נציגים שונים של $v\left(K^\times\right)$. לכן יהי $a_{i,N}$ עם ערך מינימלי בין ה-$a_{i,j}$-ים. נקבל

$$\frac{s_i}{a_{i,N}} = \sum_{j=1}^{f} \underbrace{\frac{a_{i,j}}{a_{i,N}}}_{w\geq 0}\omega_j \in \mathcal{O}_L.$$

הרדוקציה של $\frac{s_i}{a_{i,N}}$ ל-ℓ לא מתאפסת, כי יש מקדם ($j=N$) שההערכה שלו היא 0, ולכן $\frac{s_i}{a_{i,N}} \in \mathcal{O}_L^\times$. לכן בהכרח $w\left(\frac{s_i}{a_{i,N}}\right) = 0$, כלומר

$$w\left(s_i\right) = w\left(a_{i,N}\right) = v\left(a_{i,N}\right) \in v\left(K^\times\right),$$

כפי שרצינו. □

הגדרה 4.58. יהי K שדה הנזלי, ותהי L/K הרחבה סופית (למעשה, מספיק של-v תהיה הרחבה יחידה w ל-L, כדי ששדה השאריות ℓ יהיה מוגדר היטב). אומרים ש-L/K **לא מסועפת** (**unramified**), אם $[L:K] = [\ell:k]$.

אם L/K הרחבה אלגברית אינסופית, אומרים ש-L/K לא מסועפת אם היא איחוד של הרחבות סופיות לא מסועפות.

תרגיל 4.59.

א. תהי L/K הערכה לא מסועפת. אזי לכל תת-הרחבה $K \subseteq M \subseteq L$, M/K ו-L/M לא מסועפות.

ב. אם L/K ו-M/K לא מסועפות, אזי גם LM/K לא מסועפת.

מסקנה 4.60. לכל הרחבה אלגברית L/K יש תת-הרחבה לא מסועפת מקסימלית T/K. במקרה שבו $L = \overline{K}$, תת-ההרחבה הלא מסועפת המקסימלית מסומנת K^{nr}.

טענה 4.61. תהי $K\subseteq T\subseteq L$ תת-ההרחבה הלא מסועפת המקסימלית. אזי $t=\ell$.

הוכחה. יהי $\overline{\alpha}\in\ell$ עם פולינום מינימלי ספרבילי $\overline{f}\left(x\right)\in k\left[x\right]$. מעל ℓ,

$$\overline{f}\left(x\right)=\left(x-\overline{\alpha}\right)\cdot\left(\text{זר ל-}\left(x-\overline{\alpha}\right)\right).$$

תהי $f\left(x\right)\in\mathcal{O}_{K}\left[x\right]$ הרמה של $\overline{f}\left(x\right)$ מאותה מעלה (בפרט, $f\left(x\right)$ אי-פריק). מהלמה של הנזל, קיים $\alpha\in L$ שמרים את $\overline{\alpha}$. לכן

$$\left[K\left(\alpha\right):K\right]=\deg f\left(x\right)=\deg\overline{f}\left(x\right)=\left[k\left(\overline{\alpha}\right):k\right].$$

זה מראה ש-$K(\alpha)/K$ היא הרחבה לא מסועפת. מכאן $K\left(\alpha\right)\subseteq T$, ובפרט $k\left(\overline{\alpha}\right)\subseteq t$. □

הגדרה 4.62. יהי $\operatorname{char}k=p$. הרחבה סופית L/K נקראת **מתונה** (**tamely ramified**), אם $p\nmid\left[L:T\right]$. אם L/K הרחבה אלגברית אינסופית, אומרים ש-L/K מתונה אם היא איחוד של הרחבות סופיות מתונות.

משפט 4.63. L/K מתונה אם ורק אם L/K רדיקלית, כלומר

$$L=T\left(\sqrt[m_{1}]{a_{1}},\ldots,\sqrt[m_{r}]{a_{r}}\right)$$

עבור $a_{i}\in T$ ו-$p\nmid m_{i}$. במקרה הזה, נקבל שוויון $\left[L:K\right]=e\cdot f$.

הוכחה. $\boxed{\Rightarrow}$ תרגיל.

$\boxed{\Leftarrow}$ תהי L/K הרחבה מתונה. בלי הגבלת הכלליות, אפשר להניח כי $T=K$. יהיו $\omega_{1},\ldots,\omega_{r}\in w\left(L^{\times}\right)$ נציגים של הקוסטים של $v\left(K^{\times}\right)$, יהיו $m_{i}=o\left(\overline{\omega_{i}}\right)\in w(L^{\times})/v(K^{\times})$, ויהיו $\gamma_{i}\in L^{\times}$ כך ש-$w\left(\gamma_{i}\right)=w_{i}$. לפי הנוסחה להרחבה של הערכה,

$$w\left(\gamma_{i}\right)=\frac{1}{n}v\left(\mathrm{N}_{L/K}\left(\gamma_{i}\right)\right)\in\frac{1}{n}v\left(K^{\times}\right),$$

לכן $m_{i}\mid n$. כיוון ש-L/K לא מתונה, $p\nmid n$, ובפרט $p\nmid m_{i}$.

אבל אפשר למצוא $c_{i}\in K$ כך ש-$w\left(\gamma_{i}^{m_{i}}\right)=v\left(c_{i}\right)$; לכן $\gamma_{i}^{m_{i}}=c_{i}u_{i}$ עבור $u_{i}\in\mathcal{O}_{L}^{\times}$. כיוון ש-$k=\ell$ (מטענה 4.61), קיים $b_{i}\in K$ שמרים את $\overline{u_{i}}\in\ell=k$. כלומר $u_{i}=b_{i}v_{i}$ עבור $v_{i}\in\mathcal{O}_{L}^{\times}$ המקיים $v_{i}\equiv1\pmod{\mathfrak{p}_{L}}$. נתבונן בפולינום $x^{m_{i}}-v_{i}$. הרדוקציה שלו מודולו $\mathfrak{p}_{L}$ היא

$$x^{m_{i}}-1=\left(x-1\right)\cdot\left(\text{זר ל-}\left(x-1\right)\right)\in\ell\left[x\right]$$

(כאן השתמשנו בעובדה ש-$x^{m_{i}}-1$ ספרבילי; אכן, $p\nmid m_{i}$, ולכן הפולינום זר לנגזרת הפורמלית שלו $m_{i}x^{m_{i}-1}$). מהלמה של הנזל,

$$x^{m_{i}}-v_{i}=\left(x-\beta_{i}\right)\cdot\text{משהו}.$$

לכן מצאנו $\beta_{i}\in\mathcal{O}_{L}^{\times}$ כך ש-$\beta_{i}^{m_{i}}=v_{i}$.

יהי $\alpha_{i}=\frac{\gamma_{i}}{\beta_{i}}\in L^{\times}$. אזי

$$\alpha_{i}^{m_{i}}=\frac{\gamma_{i}^{m_{i}}}{\beta_{i}^{m_{i}}}=\frac{c_{i}u_{i}}{v_{i}}=c_{i}b_{i}=a_{i}\in K^{\times},$$

ומתקיים

$$w\left(\alpha_{i}\right)=w\left(\gamma_{i}\right)-\underbrace{w\left(\beta_{i}\right)}_{=0}=w\left(\gamma_{i}\right)=\omega_{i}.$$

נתבונן בשדה $L'=T\left(\sqrt[m_{1}]{a_{1}},\ldots,\sqrt[m_{r}]{a_{r}}\right)\subseteq L$. לשדה הזה יש אותו שדה שאריות כמו ל-L וגם $w\left(L\right)=w\left(L'\right)$.

תרגיל. זה מראה ש-$L = L'$.

$\square$

תהי L/K הרחבת גלואה (סופית), ותהי $G = \mathrm{Gal}(L/K)$. תהי v הערכה על K (לא בהכרח הנזלית), ותהי w הרחבה של v ל-L. לכל $\sigma \in G$, גם $w \circ \sigma$ היא הערכה על L שמרחיבה את v. למעשה,

טענה 4.64. G פועלת טרנזיטיבית על קבוצת ההרחבות של v ל-L. במילים אחרות, כל ההרחבות של v ל-L הן מהצורה $w \circ \sigma$ לאיזשהו $\sigma \in G$.

הוכחה. נניח בשלילה שלא. אזי קיימות שתי הרחבות w, w' של v ל-L כך שהקבוצות $\{w \circ \sigma\}_{\sigma \in G}$ ו-$\{w' \circ \sigma\}_{\sigma \in G}$ זרות זו לזו. לפי משפט הקירוב, קיים $\alpha \in L$ שעבורו $w \circ \sigma(\alpha) > 0$ לכל $\sigma \in G$ ו-$w' \circ \sigma(\alpha) < 0$ לכל $\sigma \in G$. לכן

$$v\left(\mathrm{N}_{L/K}(\alpha)\right) = w\left(\mathrm{N}_{L/K}(\alpha)\right) = w\left(\prod_{\sigma \in G} \sigma(\alpha)\right) = \sum_{\sigma \in G} w \circ \sigma(\alpha) > 0,$$

ומצד שני

$$v\left(\mathrm{N}_{L/K}(\alpha)\right) = w'\left(\mathrm{N}_{L/K}(\alpha)\right) = w'\left(\prod_{\sigma \in G} \sigma(\alpha)\right) = \sum_{\sigma \in G} w' \circ \sigma(\alpha) < 0$$

בסתירה. $\square$

הגדרה 4.65. תת-חבורת הפירוק (decomposition subgroup) של w הינה

$$G_w = \{\sigma \in G : w \circ \sigma = w\}.$$

הערה. נניח ש-$A \subseteq B$ תחומי דדקינד, $\mathfrak{p} \subseteq A$ אידאל ראשוני, ו-$\mathfrak{p}B = P_1^{e_1} \ldots P_r^{e_r}$. ניקח v להיות ההערכה ה-$\mathfrak{p}$-אדית. אז כל הרחבה w של v מתאימה לאיזשהו P_i, וכן $G_w = G(P_i/\mathfrak{p})$.

הערה. לכל $\sigma \in G$ מתקיים

$$\sigma G_w \sigma^{-1} = G_{w \circ \sigma} = G_{w'},$$

כלומר כל תת-חבורות הפירוק צמודות זו לזו. לכן $[G : G_w]$ הוא מספר ההרחבות של v ל-L.

יהיו $\mathcal{O}_L = \{\alpha \in L : w(\alpha) \geq 0\}$ ו-$\mathfrak{p}_L = \{\alpha \in L : w(\alpha) > 0\}$. לכל $\sigma \in G_w$ מתקיים $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ ו-$\sigma(\mathfrak{p}_L) = \mathfrak{p}_L$, לכן σ משרה $\overline{\sigma} \in \mathrm{Gal}(\ell/k)$.

טענה 4.66. תהי L/K סופית. אזי יש סדרה מדויקת

$$0 \to I_w \to G_w \xrightarrow{\varphi} \mathrm{Gal}(\ell/k) \to 0$$

כך ששדה השבת של I_w הוא T, תת-ההרחבה הלא מסועפת המקסימלית של L.

הגדרה 4.67. I_w נקראת **תת-חבורת ההתמדה / האינרציה (inrtia subgroup)**.

הוכחה. נתחיל מלהוכיח כי φ על. יהי $\overline{\sigma}\in\operatorname{Gal}\left({}^{\ell}/_{k}\right)$. ${}^{\ell}/_{k}$ ספרבילית וסופית, לכן קיים $\overline{\alpha}\in\ell$ איבר פרימיטיבי, ויהי $\overline{g}\left(x\right)\in k\left[x\right]$ הפולינום המינימלי של $\overline{\alpha}$. נבחר $\alpha\in\mathcal{O}_L^{\times}$ הרמה של $\overline{\alpha}$, ויהי $f\left(x\right)\in\mathcal{O}_K\left[x\right]$ הפולינום המינימלי של α. נשים לב כי $\overline{\sigma}\left(\overline{\alpha}\right)$ שורש של $\overline{g}\left(x\right)$, ובפרט של $\overline{f}\left(x\right)$; לכן אפשר להרים אותו לשורש $\beta\in\mathcal{O}_L^{\times}$ של $f\left(x\right)$. ${}^{L}/_{K}$ גלואה, לכן קיים $\sigma\in\operatorname{Gal}\left({}^{L}/_{K}\right)$ כך ש-$\sigma\left(\alpha\right)=\beta$. הראינו שמתקיים

$$\varphi\left(\sigma\right)\left(\overline{\alpha}\right)=\overline{\sigma}\left(\overline{\alpha}\right),$$

ולכן מהפרימיטיביות של α נקבל $\varphi\left(\sigma\right)=\overline{\sigma}$. זה מראה ש-$\varphi$ על.

כעת נרצה להראות כי תת-השדה שנקבע על ידי $\ker\varphi$ הוא T. נשים לב כי T גלואה מעל K; אכן, לכל $\sigma\in G$ מתקיים ש-${}^{\sigma(T)}/_{K}$ לא מסועפת, ומהמקסימליות של T נקבל $\sigma\left(T\right)\subseteq T$. לכן $\operatorname{Gal}\left({}^{L}/_{T}\right)\lhd G$. אבל הוכחנו ש-$t=\ell$, ולכן $\operatorname{Gal}\left({}^{L}/_{T}\right)\subseteq\ker\varphi$ (כי לכל $\sigma\in\operatorname{Gal}\left({}^{L}/_{T}\right)$, $\overline{\sigma}\in\operatorname{Gal}\left({}^{\ell}/_{t}\right)$ קובע כל איבר של t, לכן טריוויאלי). מצד שני,

$$\left|{}^{G}/_{\operatorname{Gal}\left({}^{L}/_{T}\right)}\right|=\left|\operatorname{Gal}\left({}^{T}/_{K}\right)\right|=\left[T:K\right]=\left[t:k\right]=\left[\ell:k\right]=$$
$$=\left|\operatorname{Gal}\left({}^{\ell}/_{k}\right)\right|=\left|\operatorname{Im}\varphi\right|=\left|{}^{G}/_{\ker\varphi}\right|.$$

זה מראה ש-$\left|\ker\varphi\right|=\left|\operatorname{Gal}\left({}^{L}/_{T}\right)\right|$, לכן $\operatorname{Gal}\left({}^{L}/_{T}\right)=\ker\varphi$. $\square$

הערה. נניח ש-${}^{L}/_{K}$ הרחבת גלואה אינסופית; למשל, ${}^{\overline{K}}/_{K}$. אם $K\subseteq M\subseteq L$ תת-הרחבה, ואם w הרחבה של v ל-L, אזי

$$G_w\cap\operatorname{Gal}\left({}^{L}/_{M}\right)=G_w\left({}^{L}/_{M}\right).$$

אם $K\subseteq M\subseteq E$ כולן סופיות ו-$H=\operatorname{Gal}\left({}^{E}/_{M}\right)$, מתקיים

$$\operatorname{Gal}\left({}^{E}/_{K}\right)\twoheadrightarrow\operatorname{Gal}\left({}^{M}/_{K}\right)$$

ותחת ההעתקה הזו מתקיים

$${}^{I_w\left({}^{E}/_{K}\right)H}/_{H}\rightarrow I_w\left({}^{M}/_{K}\right).$$

לכן אפשר להגדיר את תת-חבורת ההתמדה גם להרחבה אינסופית:

$$I_w\left({}^{L}/_{K}\right)=\varprojlim_{{}^{M}/_{K}\text{ finite Galois}}I_w\left({}^{M}/_{K}\right).$$

במקרה שבו $L=\overline{K}$,

$$I_w\left({}^{\overline{K}}/_{K}\right)=\operatorname{Gal}\left({}^{\overline{K}}/_{K^{\mathrm{nr}}}\right).$$

נשים לב שגם עבור תת-חבורת ההתמדה מתקיים

$$I_w\cap\operatorname{Gal}\left({}^{L}/_{M}\right)=I_w\left({}^{L}/_{M}\right)$$

לכל תת-הרחבה $K\subseteq M\subseteq L$.

תרגיל 4.68. תהי ${}^{L}/_{K}$ סופית, תהי v הערכה על K, יהי $p=\operatorname{char}k$, ותהי w הרחבה של v ל-L.

א. לחבורה I_w יש תת-חבורת p-סילו נורמלית.

ב. שדה השבת של תת-החבורה הזו הינו תת-ההרחבה המתונה המקסימלית של L.

4.9 משפט הרברנד

מעכשיו והלאה נניח ש-v_K הערכה בדידה על שדה הנזלי K.

הגדרה 4.69. v_K נקראת **מנורמלת** אם $v_K\left(K^{\times}\right)=\mathbb{Z}$.

נניח ש-v_K מנורמלת. תהי ${}^{L}\!/_{K}$ הרחבת גלואה סופית עם $G=\operatorname{Gal}\left({}^{L}\!/_{K}\right)$, ותהי w הרחבה של v_K ל-L. לכן גם w הערכה בדידה. לכל $s\geq -1$ שלם נגדיר

$$G_s=\left\{\sigma\in G_w:\forall\alpha\in\mathcal{O}_L:\sigma\left(\alpha\right)-\alpha\in\mathfrak{p}_L^{s+1}\right\}.$$

בפרט, $G_{-1}=G_w$ ו-$G_0=I_w$.

כעת יכול להיות ש-w לא מנורמלת: כיוון ש-$\pi_K\mathcal{O}_L=\mathfrak{p}_K\mathcal{O}_L=\mathfrak{p}_L^e$, מקבלים $\pi_K=u\cdot\pi_L^e$ עבור $u\in\mathcal{O}_L^{\times}$, ולכן

$$w\left(\pi_K\right)=v_K\left(\pi_K\right)=1\Longrightarrow w\left(\pi_L\right)=\frac{1}{e}.$$

זה מראה ש-$v_L=e\cdot w$ היא הערכה מנורמלת על L. כעת לכל $\alpha\in L$ מתקיים

$$v_L\left(\alpha\right)\geq m\iff\alpha\in\mathfrak{p}_L^m,$$

וזה מאפשר להגדיר את G_s לכל $s\geq -1$ ממשי:

$$G_s=\left\{\sigma\in G_w:\forall\alpha\in\mathcal{O}_L:v_L\left(\sigma\left(\alpha\right)-\alpha\right)\geq s+1\right\}.$$

נשים לב שמתקיים

$$G_s=G_{\lceil s\rceil}$$

לכל $s\geq -1$.

היינו רוצים להגדיר את G_s גם להרחבת גלואה אינסופית על ידי לקיחת הגבול ההפוך של G_s לכל תת-הרחבה סופית. הבעיה היא שזו לא בהכרח מערכת פרויקטיבית.

טענה 4.70. תהי ${}^{L}\!/_{K}$ הרחבת גלואה סופית. אזי קיים $\alpha\in\mathcal{O}_L$ כך ש-$\mathcal{O}_L=\mathcal{O}_K\left[\alpha\right]$.

הוכחה. יהי $e=e\left({}^{L}\!/_{K}\right)$. כיוון ש-${}^{\ell}\!/_{k}$ ספרבילית וסופית, קיים $\overline{\alpha}\in\ell$ כך ש-$\ell=k\left(\overline{\alpha}\right)$. יהי $\overline{g}\left(x\right)\in k\left[x\right]$ הפולינום המינימלי של $\overline{\alpha}$, ותהי $\alpha\in\mathcal{O}_L$ הרמה שלו. אם $f=f\left({}^{L}\!/_{K}\right)$, אז $1,\overline{\alpha},\ldots,\overline{\alpha}^{f-1}$ בסיס של ℓ מעל k. כפי שראינו בהוכחת טענה 4.57, $\left\{\alpha^i\pi_L^j\right\}_{0\leq i\leq f-1,0\leq j\leq e-1}$ בסיס של $\mathcal{O}_L$ כ-$\mathcal{O}_K$-מודול. נחפש π_L "טוב".

תהי $g\left(x\right)\in\mathcal{O}_K\left[x\right]$ הרמה של $\overline{g}\left(x\right)$. נשים לב ש-$\overline{g\left(\alpha\right)}=\overline{g}\left(\overline{\alpha}\right)=0$, לכן $g\left(\alpha\right)\in\mathfrak{p}_L$.

- אם $g\left(\alpha\right)$ אוניפורמיזנטה, סיימנו אם ניקח $\pi_L=g\left(\alpha\right)$.
- אחרת, אם $v_L\left(g\left(\alpha\right)\right)>1$, ניקח את $\alpha+\pi_L$ במקום את α. לפי פיתוח טיילור,

$$g\left(\alpha+\pi_L\right)=\underbrace{g\left(\alpha\right)}_{v_L>1}+g'\left(\alpha\right)\cdot\underbrace{\pi_L}_{v_L=1}+\underbrace{\cdots}_{v_L\geq 2}.$$

כיוון ש-$\overline{g}\left(x\right)$ ספרבילי, $\overline{g}'\left(\overline{\alpha}\right)\neq 0$, ומכאן $g'\left(\alpha\right)\in\mathcal{O}_L^{\times}$. לכן $v_L\left(g'\left(\alpha\right)\cdot\pi_L\right)=1$, וכיוון ששאר המחוברים עם הערכה גדולה יותר, נקבל כי $v_L\left(g\left(\alpha+\pi_L\right)\right)=1$, כלומר $g\left(\alpha+\pi_L\right)$ אוניפורמיזנטה.

□

הגדרה 4.71. תהי L/K הרחבת גלואה סופית. נגדיר

$$.\eta_{L/K}(s)=\int_0^s\frac{1}{[G_0:G_x]}\,dx$$

נסמן $g_i=|G_i|$. אם $m_i\le s<m+1$ עבור $m\in\mathbb{N}_0$, נקבל

$$.\eta_{L/K}(s)=\int_0^1+\int_1^2+\cdots+\int_{m-1}^m+\int_m^s=\frac{g_1}{g_0}+\frac{g_2}{g_0}+\cdots+\frac{g_m}{g_0}+\frac{g_{m+1}}{g_0}(s-m)$$

הגדרה 4.72. יהי $\sigma\in G$. נגדיר

$$i_{L/K}(\sigma)=v_L(\sigma(\alpha)-\alpha)$$

כאשר $\alpha\in\mathcal{O}_L$ איבר המקיים $\mathcal{O}_L=\mathcal{O}_K[\alpha]$.

אפשר לבדוק כי מתקיים

$$.i_{L/K}(\sigma)=\min\{v_L(\sigma(\beta)-\beta):\beta\in\mathcal{O}_L\}$$

לכן $i_{L/K}(\sigma)$ אינו תלוי בבחירת α. בנוסף,

$$.\sigma\in G_n\iff i_{L/K}(\sigma)\ge n+1$$

למה 4.73.

$$.\eta_{L/K}(s)=\frac{1}{g_0}\sum_{\sigma\in G}\min\left\{i_{L/K}(\sigma),s+1\right\}-1$$

הוכחה. שני האגפים הם פונקציות רציפות ולינאריות למקוטעין (ואפילו הנקודות הלא גזירות של שתי הפונקציות הן שלמות). נסמן על ידי $\theta(s)$ את האגף הימני. נשים לב כי

$$\eta_{L/K}(0)=0$$
$$\theta(0)=\frac{1}{g_0}\sum_{\sigma\in G_0}1-1=0$$

ולכן שתי הפונקציות מתחילות מאותו הערך. אם נראה שיש להן נגזרת זהה בכל נקודה לא שלמה זה יוכיח שהן שוות. ואכן, אם $m<s<m+1$ עבור $m\in\mathbb{N}_0$, אזי

$$\begin{aligned}\theta'(s)&=\frac{1}{g_0}\cdot\left|\left\{\sigma\in G:\min\left\{i_{L/K}(\sigma),s+1\right\}=s+1\right\}\right|=\\&=\frac{1}{g_0}\cdot\left|\left\{\sigma\in G:i_{L/K}(\sigma)\ge s+1\right\}\right|=\\&=\frac{1}{g_0}\cdot\left|\left\{\sigma\in G:i_{L/K}(\sigma)\ge\lceil s\rceil+1\right\}\right|=\frac{1}{g_0}\cdot g_{m+1}=\eta'_{L/K}(s)\end{aligned}$$

זה מראה את השוויון הדרוש. □

משפט 4.74 (משפט הרברנד). יהי $K \subseteq L' \subseteq L$ מגדל של הרחבות גלואה סופיות, ותהי $H = \operatorname{Gal}\left({}^{L}/_{L'}\right)$, כלומר $\operatorname{Gal}\left({}^{L'}/_{K}\right) \cong {}^{G}/_{H} = G'$. אזי ההטלה במערכת הפרויקטיבית $G \twoheadrightarrow {}^{G}/_{H}$ מקיימת

$$ {}^{G_s H}/_{H} = G'_{\eta_{L/L'}(s)}. $$

מסקנה 4.75. תהי $\psi_{L/K}$ הפונקציה ההופכית של $\eta_{L/K}$. נגדיר $G^t = G_{\psi_{L/K}(t)}\left({}^{L}/_{K}\right)$. אזי

$$ {}^{G^t H}/_{H} = \left(G'\right)^t, $$

ולכן אפשר להגדיר

$$ G_K^t = \varprojlim_{{}^{L}/_{K} \text{ finite Galois}} G^t\left({}^{L}/_{K}\right) \leq G_K. $$

הוכחת משפט הרברנד. יהי $\sigma' \in G'$, ותהי $\sigma \in G$ הרמה כך ש-$i_{L/K}(\sigma)$ מקסימלי.

טענה. $i_{L'/K}(\sigma') = \eta_{L/L'}\left(i_{L/K}(\sigma) - 1\right) + 1$.

מטענת העזר נקבל

$$ \sigma' \in {}^{G_s H}/_{H} \iff \text{ל-}\sigma'\text{ יש מקור ב-}G_s \iff i_{L/K}(\sigma) \geq s+1 \iff $$
$$ \iff i_{L/K}(\sigma) - 1 \geq s \iff \eta_{L/L'}\left(i_{L/K}(\sigma) - 1\right) \geq \eta_{L/L'}(s) \iff $$
$$ \iff i_{L'/K}(\sigma') \geq \eta_{L/L'}(s) \iff \sigma' \in G'_{\eta_{L/L'}(s)} $$

$\square$

משפט (האסה-ארף, 1939). אם ${}^{L}/_{K}$ סופית ואבלית, אזי הקפיצות ב-G^t (כלומר $G^t \supsetneq G^{t+\varepsilon}$ לכל $\varepsilon > 0$) קורות רק ב-t-ים שלמים. אם ${}^{L}/_{K}$ לא אבלית, יכולות להיות קפיצות גם בנקודות לא שלמות.

5 הקדמה לתורת שדות המחלקות

תהי ${}^{K}/_{\mathbb{Q}_p}$ הרחבה סופית, ותהי ${}^{L}/_{K}$ הרחבת גלואה. אפשר למצוא שדות מספרים ${}^{M}/_{F}$ ואידאלים ראשוניים $\mathfrak{p} \subseteq \mathcal{O}_F$ ו-$P \subseteq \mathcal{O}_M$ כך ש-$\mathfrak{p} \mid P$, שעבורם $K = F_{\mathfrak{p}}$ ו-$L = M_P$. מקבלים סדרה מדויקת

$$ 1 \to I\left({}^{L}/_{K}\right) \to \operatorname{Gal}\left({}^{L}/_{K}\right) \to \operatorname{Gal}\left({}^{\ell}/_{k}\right) \to 1. $$

נשים לב ש-$\operatorname{Gal}\left({}^{L}/_{K}\right)$ היא תת-חבורת הפירוק, כי $\mathbb{Q}_p$ הנזלי. בנוסף, ${}^{\ell}/_{k}$ הרחבה של שדות סופיים, לכן החבורה $\operatorname{Gal}\left({}^{\ell}/_{k}\right)$ היא ציקלית.

"נשאיף $L \to \infty$", כלומר ניקח את הגבול ההפוך, ונקבל

$$ 1 \to I_K \to G_K \xrightarrow{\pi} G_k \to 1. $$

נשים לב שמתקיים

$$ G_k = \varprojlim_{{}^{\ell}/_{k} \text{ finite}} \operatorname{Gal}\left({}^{\ell}/_{k}\right) $$

כשכל $\operatorname{Gal}\left({}^{\ell}/_{k}\right)$ ציקלית ונוצרת על ידי אוטומורפיזם פרובניוס: $\operatorname{Frob}_k : x \mapsto x^q$ עבור $q = |k|$. G_k היא לא ציקלית, אבל היא כן ציקלית טופולוגית, כלומר $\langle \operatorname{Frob}_k \rangle$ תת-חבורה צפופה של G_k.

הגדרה 5.1. תת-חבורת וייל (Weil subgroup) הינה

$$W_K = \left\{\sigma \in G_K : \pi(\sigma) \in \langle \mathrm{Frob}_k \rangle\right\}.$$

לכן $W_K \subseteq G_K$ תת-חבורה צפופה.

תהי $H \subseteq G_K$ תת-חבורה. נסמן את האבליניזציה של G_K על ידי

$$G_K^{\mathrm{ab}} = {}^{G_K}\!/\!_{[G_K, G_K]},$$

ונסמן על ידי H^{ab} את התמונה של H ב-G_K^{ab}.

משפט 5.2 (הוכיחו *Artin* ו-*Hasse*, מסביבות 1930)**.** קיים איזומורפיזם

$$\begin{array}{ccccc}
\mathbb{Z} \times \mathcal{O}_K^{\times} & = & K^{\times} \xrightarrow{\sim} W_K^{\mathrm{ab}} & & \\
 & & \cup\!\!\!\mid \qquad\quad \cup\!\!\!\mid & & \\
 & & \mathcal{O}_K^{\times} \xrightarrow{\sim} I_K^{\mathrm{ab}} & = & G_0^{\mathrm{ab}} \\
 & & \cup\!\!\!\mid \qquad\quad \cup\!\!\!\mid & & \\
 & & 1 + \mathfrak{p}_K^n \xrightarrow{\sim} \left(G^n\right)^{\mathrm{ab}} & &
\end{array}$$

כדי להוכיח את המשפט הזה, צריך להשתמש בכלים של קוהומולוגיה.

5.1 מבוא לקוהומולוגיה של חבורות

תהי G חבורה טופולוגית, ויהי M **G-מודול**, כלומר G פועלת על החבורה האבלית M, והמייצב $\mathrm{stab}(m)$ פתוח ב-G לכל $m \in M$. נגדיר

$$C^i(G, M) = \left\{\psi : G^i \to M : \text{קבועה מקומית}\ \psi\right\}$$

והעתקות $d^i : C^i(G, M) \to C^{i+1}(G, M)$, שנקראות **העתקות שפה (boundary maps)**, על ידי

$$\begin{aligned}
\left(d^i \psi\right)(x_1, \ldots, x_{i+1}) = x_1 \cdot \psi(x_2, \ldots, x_{i+1}) - \psi(x_1 x_2, x_3, \ldots, x_{i+1}) + \\
+ \psi(x_1, x_2 x_3, x_4, \ldots, x_{i+1}) - \cdots + \\
+ (-1)^i \cdot \psi(x_1, \ldots, x_{i-1}, x_i x_{i+1}) + (-1)^{i+1} \cdot \psi(x_1, \ldots, x_i)
\end{aligned}$$

אפשר לוודא כי $d^{i+1} \circ d^i = 0$ לכל i, כלומר $\mathrm{Im}\, d^i \subseteq \ker d^{i+1}$. מגדירים את **חבורת הקוהומולוגיה מסדר** i לפי

$$H^i(G, M) = {}^{\ker d^i}\!/\!_{\mathrm{Im}\, d^{i+1}}.$$

ניתן לבנות את הקוהומולוגיה גם כפונקטור הנגזר של פונקטור ה-G-אינווריאנטים,

$$M \mapsto M^G = \{m \in M : \forall g \in G : gm = m\}.$$

בפירוט: ניקח רזולוציה אינג'קטיבית

$$0 \to M \to I_0 \to I_1 \to I_2 \to \cdots$$

שהיא סדרה מדויקת. אחרי שנפעיל את פונקטור ה-G-אינווריאנטים, נקבל קומפלקס

$$0 \to M^G \to I_0^G \xrightarrow{d^0} I_1^G \xrightarrow{d^1} I_2^G \xrightarrow{d^2} \cdots$$

שאינו בהכרח סדרה מדויקת. אז מתקיים

$$.H^i(G,M) = {}^{\ker d^i}/_{\operatorname{Im} d^{i+1}}$$

בהינתן סדרה מדויקת קצרה

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

מקבלים סדרה מדויקת ארוכה

$$0 \to H^0(G,M_1) \to H^0(G,M_2) \to H^0(G,M_3) \to H^1(G,M_1) \to H^1(G,M_2) \to H^1(G,M_3) \to H^2(G,M_1) \to \cdots$$

איך מחשבים את H^0 ואת H^1?

חישוב H^0. במקרה הזה,

$$,C^0(G,M) = \{\text{פונקציות קבועות}\} = M$$
$$,\left(d^0 m\right)(g) = gm - m$$

ולכן

$$.H^0(G,M) = M^G$$

חישוב H^1. במקרה הזה,

$$C^1(G,M) = \{\psi : G \to M\}$$

וכן

$$.\left(d^1\psi\right)(g_1,g_2) = g_1\psi(g_2) - \psi(g_1g_2) + \psi(g_1)$$

אז

$$.\ker d^1 = \{\psi : G \to M : \psi(g_1g_2) = \psi(g_1) + g_1\psi(g_2)\}$$

כל ψ כזה נקרא **הומומורפיזם מפותל** (**crossed homomorphism**).

דוגמה 5.3. ניקח $K/\mathbb{Q}_p$ כנ"ל. נקבל סדרה של G_K-מודולים לפי

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow[x\mapsto x^n]{} \overline{K}^\times \longrightarrow 1\,,$$

ומהסדרה המדויקת הארוכה נקבל

$$\begin{array}{ccccccc}
H^0\left(G_K,\overline{K}^\times\right) & \longrightarrow & H^0\left(G_K,\overline{K}^\times\right) & \longrightarrow & H^1\left(G_K,\mu_n\right) & \longrightarrow & H^1\left(G_K,\overline{K}^\times\right) \\
\parallel & & \parallel & & & & \parallel \\
K^\times & \xrightarrow[x\mapsto x^n]{} & K^\times & & & & 0
\end{array}$$

כאשר $H^1\left(G_K,\overline{K}^\times\right)=0$ לפי הילברט 90. לכן

$$H^1\left(G_K,\mu_n\right)\cong K^\times/\left(K^\times\right)^n.$$

5.2 דוגמת שימוש: חבורת בראוור של הרחבות של $\mathbb{Q}_p$

תהי L/K הרחבת שדות. יש הומומורפיזם $\mathrm{Br}(K)\to\mathrm{Br}(L)$ לפי $[A]\mapsto[A\otimes_K L]$. נסמן על ידי $\mathrm{Br}(L/K)$ את הגרעין של ההומומורפיזם; הוא נקרא **חבורת בראוור היחסית** של L מעל K. למשל, $\mathrm{Br}\left(\overline{K}/K\right)=\mathrm{Br}(K)$.

מסתבר שיש קשר חזק בין חבורת בראוור לקוהומולוגיה: מתקיים

$$\mathrm{Br}(L/K)\cong H^2\left(\mathrm{Gal}(L/K),L^\times\right).$$

בפרט, נקבל את השוויון

$$\mathrm{Br}(K)=\mathrm{Br}\left(\overline{K}/K\right)\cong H^2\left(G_K,\overline{K}^\times\right).$$

במקרה שבו $K/\mathbb{Q}_p$ הרחבת גלואה סופית, אפשר לתת תיאור מלא של $\mathrm{Br}(K)$. ישנה סדרה מדויקת

$$1\longrightarrow L^\times\longrightarrow \mathrm{GL}_n(L)\longrightarrow \mathrm{PGL}_n(L)\longrightarrow 1\,.$$

הבעיה היא שהחבורות האלו אינן אבליות לכל $n\geq 2$, והקוהומולוגיה לא תצא חבורה אלא רק קבוצה מנוקדת (pointed set). לכן צריך לבצע עיקוף.

טענה 5.4. לכל A/K פשוטה מרכזית קיימת הרחבה לא מסועפת סופית L/K שעבורה

$$A\otimes_K L\cong \mathrm{M}_n(L).$$

רעיון ההוכחה. לכל $\alpha\in A$ נגדיר $|\alpha|$ באופן הבא: נחשוב על α כאופרטור $M_\alpha:A\to A$ שכופל ב-α משמאל, וניקח $|\alpha|=|\det M_\alpha|$. עם קצת מאמץ, $|\cdot|$ היא הערכה לא ארכימדית על A. כפי שעשינו במקרה הקומוטטיבי, אפשר להגדיר

$$\mathcal{O}_A=\{\alpha\in A:|\alpha|\leq 1\}\,,$$
$$\mathfrak{p}_A=\{\alpha\in A:|\alpha|<1\}\subseteq\mathcal{O}_A.$$

אז $\ell=\mathcal{O}_A/\mathfrak{p}_A=k\left[\overline{\delta}\right]$ לאיזשהו $\delta\in\mathcal{O}_A$, ומקבלים ש-$L=K(\delta)\subseteq A$ תת-שדה מקסימלי לא מסועף. לכן L מפצל את A, כלומר $A\otimes_K L\cong\mathrm{M}_n(L)$. $\square$

מסקנה 5.5.

$$\mathrm{Br}(K) = \mathrm{Br}\left({}^{K^{\mathrm{nr}}}\!/\!{}_{K}\right) \cong H^2\left(\mathrm{Gal}\left({}^{K^{\mathrm{nr}}}\!/\!{}_{K}\right), \left(K^{\mathrm{nr}}\right)^{\times}\right).$$

כיוון שמתקיים

$$\mathrm{Gal}\left({}^{K^{\mathrm{nr}}}\!/\!{}_{K}\right) \cong {}^{G_K}\!/\!{}_{I_K} \cong G_k,$$

נקבל

$$\mathrm{Br}(K) \cong H^2\left(G_k, \left(K^{\mathrm{nr}}\right)^{\times}\right).$$

משפט 5.6. $\mathrm{Br}(K) = {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}}$.

ניתן את רעיון ההוכחה. לוליואציה המנורמלת v_K יש הרחבה יחידה w ל-L, ואנחנו יודעים ש-$v_L = e \cdot v_K$. במקרה שבו $e = 1$, כלומר ${}^{L}\!/\!{}_{K}$ לא מסועפת, v_L היא ממש הרחבה של v_K. יש סדרה מדויקת

$$1 \longrightarrow \mathcal{O}_{K^{\mathrm{nr}}}^{\times} \longrightarrow \left(K^{\mathrm{nr}}\right)^{\times} \xrightarrow{v_K} \mathbb{Z} \longrightarrow 1,$$

ולכן יש הומומורפיזם

$$\mathrm{Br}(K) \cong H^2\left(G_k, \left(K^{\mathrm{nr}}\right)^{\times}\right) \to H^2\left(G_k, \mathbb{Z}\right).$$

לכן נרצה להבין את $H^2\left(G_k, \mathbb{Z}\right)$. נסתכל על הסדרה המדויקת

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}} \longrightarrow 0$$

שבה הפעולה של G_k טריוויאלית. אז

$$\begin{array}{ccccccc} H^1\left(G_k, \mathbb{Q}\right) & \longrightarrow & H^1\left(G_k, {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}}\right) & \xrightarrow{\sim} & H^2\left(G_k, \mathbb{Z}\right) & \longrightarrow & H^2\left(G_k, \mathbb{Q}\right) \\ \parallel & & & & & & \parallel \\ 0 & & & & & & 0 \end{array}$$

בנוסף, יש איזומורפיזם

$$H^1\left(G_k, {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}}\right) = \mathrm{Hom}_{\mathrm{cont}}\left(G_k, {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}}\right) \xrightarrow[\psi \mapsto \psi(\mathrm{Frob}_k)]{\sim} {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}}.$$

נרכיב את כל ההעתקות שקיבלנו:

$$\mathrm{Br}(K) \xrightarrow{\sim} H^2\left(G_k, \left(K^{\mathrm{nr}}\right)^{\times}\right) \xrightarrow[v_K]{\sim} H^2\left(G_k, \mathbb{Z}\right) \xrightarrow{\sim} H^1\left(G_k, {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}}\right) \xrightarrow{\sim} {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}},$$

ולכן $\mathrm{Br}(K) \cong {}^{\mathbb{Q}}\!/\!{}_{\mathbb{Z}}$.

5.3 דואליות פואנקרה

יהי M G-מודול סופי, ויהי $i \in \{0,1,2\}$. ניקח $\mu_\infty \subseteq \overline{K}^\times$ כאוסף כל שורשי היחידה ב-$\overline{K}^\times$, ונגדיר

$$M^* = \operatorname{Hom}(M, \mu_\infty).$$

M^* הוא G_K-מודול לפי

$$\forall \sigma \in G_K\, \forall f \in M^* : (\sigma f)(m) = \sigma\left(f\left(\sigma^{-1}(m)\right)\right).$$

כחבורה מופשטת, $\mu_\infty \cong \mathbb{Q}/\mathbb{Z}$. נשים לב שיש העתקה $M \otimes_K M^* \to \mu_\infty$ לפי $m \otimes f \mapsto f(m)$. ההעתקה משרה סדרה

$$H^i(G_K, M) \times H^{2-i}(G_K, M^*) \xrightarrow[\text{cup product}]{\cup} H^2(G_K, M \otimes_K M^*) \longrightarrow H^2(G_K, \mu_\infty) \longrightarrow$$
$$\xrightarrow[\mu_\infty \hookrightarrow \overline{K}^\times]{} H^2\left(G_K, \overline{K}^\times\right) \cong \operatorname{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$$

טענה 5.7. הזיווג $(\varphi, \psi) \mapsto \langle \varphi, \psi \rangle \in \mathbb{Q}/\mathbb{Z}$ הוא **זיווג מושלם**.

אם A חבורה אבלית, מגדירים את **הדואלי של פונטריאגין** להיות

$$A^\vee = \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z}).$$

הזיווג $(\varphi, \psi) \mapsto \langle \varphi, \psi \rangle$ משרה שתי העתקות: הראשונה היא

$$H^i(G_K, M) \to \left(H^{2-i}(G_K, M^*)\right)^\vee$$
$$\varphi \mapsto (\psi \mapsto \langle \varphi, \psi \rangle)$$

והשנייה בדומה:

$$H^{2-i}(G_K, M^*) \to \left(H^i(G_K, M)\right)^\vee$$
$$\psi \mapsto (\varphi \mapsto \langle \varphi, \psi \rangle)$$

"זיווג מושלם" פירושו ששתי ההעתקות האלו הן איזומורפיזמים.

אם כן,

$$\left(G_K^{\text{ab}}\right)^\vee = \operatorname{Hom}\left(G_K^{\text{ab}}, \mathbb{Q}/\mathbb{Z}\right) = \operatorname{Hom}(G_K, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}\left(G_K, \varinjlim \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}\right) =$$
$$= \varinjlim \operatorname{Hom}(G_K, \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}) = \varinjlim H^1(G_K, \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}) = (\star)$$

מהדואליות של פואנקרה, אם $M = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, נקבל $H^1(G_K, M) \cong \left(H^1(G_K, M^*)\right)^\vee$.

נוסף על כך, מתקיים

$$M^* = \operatorname{Hom}(\tfrac{1}{n}\mathbb{Z}/\mathbb{Z}, \mu_\infty) = \mu_n.$$

לכן

$$(\star) = \varinjlim \left(H^1(G_K, M^*)\right)^\vee = \varinjlim \left(H^1(G_K, \mu_n)\right)^\vee = \varinjlim \left(K^\times/(K^\times)^n\right)^\vee = \left(K^\times\right)^\vee.$$

תרגיל 5.8. תהי A חבורה אבלית כך ש-A/nA סופי לכל n. אזי $(A^\vee)^\vee = \varprojlim A/nA$.

בסך הכל נקבל איזומורפיזם

$$.G_K^{\mathrm{ab}} \cong \varprojlim K^\times/(K^\times)^n = \widehat{K^\times}$$

$K^\times \subseteq \widehat{K^\times}$ היא תת-חבורה. מסתבר שתת-החבורה המתאימה ב-G_K^{ab} היא W_K^{ab}, כלומר הן איזומורפיות.

תהי L/K הרחבה סופית כך ש-$\overline{L} = \overline{K}$; אזי $G_L \subseteq G_K$. נקבל דיאגרמה קומוטטיבית

$$\begin{array}{ccc} K^\times & \xrightarrow{\sim} & W_K^{\mathrm{ab}} \\ {\scriptstyle \mathrm{N}_{L/K}} \uparrow & & \uparrow \\ L^\times & \xrightarrow{\sim} & W_L^{\mathrm{ab}} \end{array}$$

לכן, אם L/K אבלית,

$$.\mathrm{Gal}\left(L/K\right) \cong K^\times/\mathrm{N}_{L/K}\left(L^\times\right)$$

זה מאפשר לנו להבין את ההרחבות האבליות של K, אבל לא עוזר בהבנת ההרחבות הלא אבליות.

5.4 תוכנית לנגלנדס

מתקיים

$$\text{הצגות חד-מימדיות של } G_K = \mathrm{Hom}\left(G_K, F^\times\right) = \mathrm{Hom}\left(G_K^{\mathrm{ab}}, F^\times\right)$$

ומצד שני

$$\text{הצגות חד-מימדיות של } K^\times = \mathrm{Hom}\left(K^\times, F^\times\right) \text{ ”} = \text{“ } \mathrm{Hom}\left(G_K^{\mathrm{ab}}, F^\times\right).$$

לנגלנדס העלה השערה שלפיה יש גם התאמה במימדים גדולים יותר:

$$\text{הצגות } n\text{-מימדיות אי-פריקות של } GL_n\left(K\right) \longleftrightarrow \text{הצגות } n\text{-מימדיות אי-פריקות של } G_K.$$

אם $K/\mathbb{Q}_p$ סופית ו-$F = \mathbb{C}$, זה ידוע (Harris-Taylor, 1999). Scholze הוכיח זאת ב-2011 בדרך קצרה ופשוטה יותר.