סמינר

הקדמה

חוק ההדדיות הריבועית קובע שאם p, q ראשוניים אי זוגים ושונים אז עבור סימן לז'נדר (Legendre) שלהם

$$(p/q) = \begin{cases} 1 & n^2 = q \mod p \text{-קיים n טבעי כך ש} \\ -1 & \text{אחרת} \end{cases}$$

מתקיים

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

את החוק הזה ניתן להוכיח באמצעות החוג $\mathbb{Z}$ והשדה $\mathbb{Q}$, שתורת המספרים מתחילה מחקירתם. בהמשך התפתחו חוקי הדדיות נוספים שדרשו חוגים ושדות נוספים - למשל כדי להוכיח את חוק ההדדיות הדו ריבועית גאוס (Gauss) נזקק לחוג $\mathbb{Z}[i]$, שקרוי כיום על שמו.
לאחר ההוכחה של מספר חוקים כאלה באמצעות כמה חוגים ושדות נמצא מכנה משותף לחוגים ולשדות האלה, וכך הוגדרה הכללה שלהם: השדות הם שדות מספרים והחוגים הם חוגי השלמים שלהם. בעבודה נחקור את ההכללה הזאת ונוכיח באמצעותה את חוק ההדדיות של אייזנשטיין (Eisenstein) , הכללה חלקית אך חשובה של חוקי ההדדיות מסדרים מסוימים.
בנוסף לחשיבותו כהכללה הוא מהווה מרכיב חשוב בהוכחה של משפטים אחרים בתורת המספרים.
בסעיף 1 נגדיר את המושגים הבסיסיים שנוגעים לשדות מספרים ונוכיח את התכונות שלהם. נזדקק למונחים האלה בשארית העבודה.
בסעיף 2 נביט בשדות ריבועיים וציקלוטומיים - שדות מספרים שמתקבלים בדרך מסוימת ושיש להם חשיבות רבה להוכחת חוק ההדדיות של אייזנשטיין.
בסעיף 3 ננסח את חוק ההדדיות ונשתמש בכלים שבנינו על מנת להוכיח את יחס שטיקלברגר (Stickelberger) , משפט חשוב בפני עצמו, שבאמצעותו נוכיח לבסוף את חוק ההדדיות. בסוף הסעיף נציג מספר שימושים מעניינים של החוק.

1 תורת המספרים האלגבריים

1.1 מושגים אלגבריים

בסעיף זה ננסח ונוכיח מספר טענות אלגבריות שנצטרך בהמשך. במהלך הסעיף $K \subset L$ תהיה הרחבת שדות סופית ואלגברית. נסמן $[L:K]=n$.

הגדרה 1.1.1. *יהי $\alpha \in L$. נסמן ב-$T_\alpha : L \to L$ את ההעתקה הלינארית $T_\alpha x = \alpha x$. הנורמה של α היא $N_{L/K}(\alpha) = \det T_\alpha$, והעקבה של α היא $t_{L/K}(\alpha) = \ tr\, T$.*

מכיוון שההרחבה L/K קבועה, נשמיט בהמשך את האינדקסים התחתונים בסימוני הנורמה והעקבה. מאחר ש-$T_{\alpha+\beta} = T_\alpha + T_\beta$ ו-$T_\alpha T_\beta = T_{\alpha\beta}$ נקבל את התכונות הבאות לכל $a \in K$ מתכונות העקבה (של העתקות) והדטרמיננטה:

1. $N(\alpha\beta) = N(\alpha)N(\beta)$.
2. $t(\alpha+\beta) = t(\alpha)+t(\beta)$.
3. $N(a\beta) = a^n N(\beta)$.
4. $t(a\alpha) = at(\alpha)$.

טענה 1.1.2. *אם K סופי או בעל אפיין 0 אז t אינה זהותית 0.*

הטענה הזו נכונה לכל L/K ספרבילית, אך לא נזדקק לה. נוכל להוכיח אותה לאחר שנבסס עוד מספר תכונות של העקבה.

טענה 1.1.3. *נניח ש-L/K ספרבילית. יהי F שדה הרחבה סגור אלגברית של K. אז יש n מונומורפיזמים $\sigma_1, \ldots, \sigma_n$ של L ל-F ששומרים על K.*

הוכחה. יהי $\alpha \in L$ שהפולינום המינימלי שלו הוא ממעלה n (קיים כזה כי L הרחבה פשוטה בתור הרחבה ספרבילית סופית). כזכור מהקורס בתורת גלואה לכל שורש של הפ"מ של α יש מונומורפיזם ששומר על K ושמעביר את α אליו. ב-F הפ"מ מתפרק לגורמים לינאריים שונים כי ההרחבה ספרבילית, לכן המונומורפיזמים האלה שונים זה מזה, כלומר יש לפחות n מונומורפיזמים ששומרים על K. מצד שני כל מונומורפיזם ששומר על K חייב להעביר את α לשורש אחר של הפ"מ שלו, לכן הוא אחד מהמונומורפיזמים שהצגנו, ומכאן שיש בדיוק n כאלה. $\square$

הגדרה 1.1.4. *הצמודים של $\alpha \in L$ הם $\alpha^{(i)} = \sigma_i(\alpha)$ כאשר $\sigma_1, \ldots, \sigma_n$ הם המונומורפיזמים של L לשדה הרחבה סגור אלגברית של K ששומרים על K.*

טענה 1.1.5.

$$t(\alpha) = \sum \alpha^{(i)},$$

$$N(\alpha) = \prod \alpha^{(i)}$$

הוכחה. יהי $a \in L$ ותהי $T : L \to L$ ההעתקה $Tx = ax$. יהי $m(x) = x^k + \sum a_i x^i$ הפולינום המינימלי של a ויהי (v_i) בסיס ל-$L/K(a)$. נסמן $L_i = \text{span}\{v_i, v_i a, \dots, v_i a^{k-1}\}$ ונתייחס אליו כמרחב מעל K. זה תת מרחב T שמור והקבוצה הפורשת היא בסיס ל-L_i כי אחרת a מאפס פולינום ממעלה $k-1$. בבסיס הזה הצמצום של T ל-L_i מיוצג ע"י

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{k-1} \end{pmatrix}$$

הפולינום האופייני של המטריצה הזו הוא m.
איחוד הקבוצות הפורשות של ה-L_i הוא בגודל $[L:K] = [L:K(a)]k$ וכל $x \in L$ שווה ל-$\sum v_i x_i, x_i \in K(a)$ ששווה ל-$\sum v_i p_i(a), p \in K[x], \deg p < k$ וזו הצגה כצירוף לינארי של איחוד הקבוצות הפורשות. מכאן שאיחוד הקבוצות הפורשות הוא בסיס ל-L, כלומר $L = \bigoplus L_i$. מכאן שהפולינום האופייני של T שווה ל-$m^{[L:K(a)]}$.
נרשום $m(x) = \prod (x - \sigma_i(a))$ כאשר המכפלה היא על k אינדקסים שמייצגים את כל $\{\sigma_i(a)\}$, בה"כ $1, 2, \dots, k$. יהי $1 \le i \le k$. כמו בהוכחת טענה 1.1.3 יש בדיוק $[L:K(a)] = n/k$ מונומורפיזמים $L \to F$ שמזדהים עם σ_i על $K(a)$, נניח $\sigma_{i_1}, \dots, \sigma_{i_{n/k}}$. מכאן ש

$$(x - \sigma_i(a))^{n/k} = \prod_{j=1}^{n/k} (x - \sigma_{i_j})$$

כלומר הפולינום האופייני של T הוא $\prod_{i=1}^n (x - \sigma_i(a)) = \prod_{i=1}^k \prod_{l=1}^{n/k} (x - \sigma_{i_j}) = m(x)^{n/k}$.
הטענה נובעת מכך שהעקבה היא סכום הע"ע והדטרמיננטה היא מכפלתם. $\square$

הוכחה של טענה 1.1.2. אם $\text{Char}K = 0$ אז $t(1) = n \neq 0$. אם K סופי נקבל מטענה 1.1.5 ש-$t(x) = x + x^p + \dots + x^{p^{n-1}}$, כי המונומורפיזמים הם $0 \le i \le n-1, \sigma_i(x) = x^{p^i}$. נניח בשלילה שהם לא שונים זה מזה, כלומר לכל x מתקיים $x^{p^i} = x^{p^j}$ עבור $0 \le i < j \le n-1$. אז $(x^{p^i})^{p^{j-i}-1} = 1$, ומאחר ש-$\sigma_i$ על נקבל שלכל y מתקיים $y^{p^{j-i}-1} = 1$. זה בפרט נכון ליוצר y של החבורה הכפלית (הציקלית) של L, לכן $p^n | p^{j-i} - 1$ ומכאן ש $n \le j - i$, וזה לא ייתכן.
כעת ל-$t(x)$ יש לכל היותר p^{n-1} שורשים ומאחר שב-L יש p^n איברים היא לא זהותית 0. $\square$

הגדרה 1.1.6. *הדיסקרימיננטה של* $\alpha_1, \dots, \alpha_n \in L$ *היא*

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(t(\alpha_i \alpha_j))$$

טענה 1.1.7. *אם הדיסקרימיננטה של* (α_i) *שונה מ-0 אז* (α_i) *בסיס ל-*L/K*. אם* L/K *הרחבה ספרבילית ו-*(α_i) *בסיס שלה אז הדיסקרימיננטה של* (α_i) *אינה 0.*

הוכחה. נניח ש-(α_i) לא בסיס, כלומר $\sum a_i\alpha_i = 0$ עבור $a_i \in K$ שלא כולם 0. אז לכל j מתקיים $\sum_i a_i\alpha_i\alpha_j = 0$ ולכן $\sum_i a_i t(\alpha_i\alpha_j) = 0$. מכאן שעמודות המטריצה $(t(\alpha_i, \alpha_j))$ ת"ל ולכן הדטרמיננטה שלה היא 0, כלומר הדיסקרימיננטה של (α_i) היא 0.
נניח בשלילה ש-(α_i) בסיס שהדיסקרימיננטה שלו היא 0. נסמן $A = (t(\alpha_i, \alpha_j))$, אז העמודות של A ת"ל ולכן יש $a_i \in K$ שלא כולם 0 כך שלכל j מתקיים

$$\sum_i a_i t(\alpha_i\alpha_j) = 0$$

נסמן $\alpha = \sum a_i\alpha_i \neq 0$. אז לכל j מתקיים $t(\alpha\alpha_j) = t(\sum_i a_i\alpha_i\alpha_j) = 0$. מאחר ש-$(\alpha_i)$ בסיס ו-t לינארית נקבל ש-$t(\alpha\beta) = 0$ לכל $\beta \in L$, ולכן לכל $\beta \in L$ מתקיים $t(\beta) = t(\alpha\beta/\alpha) = 0$ כלומר t זהותית 0 ולכן ההרחבה לא ספרבילית, וזה לא ייתכן. $\square$

טענה 1.1.8. *יהיו $(\alpha_i), (\beta_i)$ שני בסיסים ל-L/K. נגדיר העתקה לינארית T לפי $T(\beta_i) = \alpha_i$. אז*

$$\Delta((\alpha_i)) = (\det T)^2\Delta((\beta_i))$$

הוכחה. מתקיים $\alpha_i = \sum_j a_{ij}\beta_j$ כאשר (a_{ij}) המטריצה המייצגת של T לפי (β_i). מכאן ש

$$\alpha_i\alpha_k = \sum_j\sum_l a_{ij}a_{kl}\beta_j\beta_l$$

ולכן $t(\alpha_i\alpha_k) = \sum_j\sum_l t(a_{ij})t(a_{kl})t(\beta_j\beta_l)$. נסמן $A = (t(\alpha_i\alpha_j)), B = (t(\beta_j\beta_l)), C = (a_{ij})$ ונקבל ש-$A = C^tBC$. מכאן ש-

$$\Delta((\alpha_i)) = |C|^2\Delta((\beta_i))$$

$\square$

טענה 1.1.9. *אם L/K ספרבילית ו-$\sigma_1, \ldots, \sigma_n$ הם המונומורפיזמים של L לשדה הרחבה סגור אלגברית של K ששומרים על K אז*

$$\Delta((\alpha_i)) = \det(\sigma_j(\alpha_i))^2$$

הוכחה. $t(\alpha_i\alpha_j) = \sum\alpha_i^{(l)}\alpha_j^{(l)}$ כלומר $A = BB^t$ כאשר $A = (t(\alpha_i\alpha_j)), B = (\alpha_i^{(j)})$, לכן $\Delta((\alpha_i)) = |B|^2$. $\square$

אם A, B אידאלים בחוג חילופי סכומם הוא $A + B = \{a + b : a \in A, b \in B\}$, ומכפלתם AB היא האידאל שנוצר ע"י $\{ab : a \in A, b \in B\}$, כלומר $AB = \{\sum a_ib_i : a_i \in A, b_i \in B\}$. הפעולות האלו קיבוציות, לכן ניתן להרחיב אותן למספר (סופי) כלשהו של אידאלים.

טענה 1.1.10. *יהי R חוג חילופי עם יחידה ויהיו (A_i) אידאלים עבורם $A_i + A_j = R$ לכל $i \neq j$. אז*
1. *לכל j יש u_j כך ש $u_j - 1 \in A_j$ ולכל $i \neq j$ $u_j \in A_i$*
2. *$\cap A_i = \prod A_i$*
3. *$R/\prod A_i \cong \bigtimes R/A_i$.*

הוכחה. נגדיר $\phi : R \to \bigtimes R/A_i$ ע"י $\phi(r) = (r + A_1, \ldots, r + A_n)$.

1. לכל i ולכל $j \neq i$ יש $x_j \in A_i, y_j \in A_j$ כך ש-$x_j + y_j = 1$. נסמן $u_i = \prod_{j\neq i} y_j = \prod(1-x_j)$, אז $u_i \in A_j$ לכל $j \neq i$ ו-$u_i - 1 \in A_i$ מאחר ש-$1 - x_j - 1 \in A_i$ לכל $j \neq i$. בכך הוכחנו את 1, ובנוסף $\phi(u_i) = e_j$ לכן ϕ על.
2. נוכיח את הטענה באינדוקציה. אם $n = 1$ התוצאה ברורה. אם $n = 2$ אז

$$A_1 \cap A_2 = (A_1 + A_2)(A_1 \cap A_2) = A_1(A_1 \cap A_2) + A_2(A_1 \cap A_2) \subset A_1A_2$$

ומאחר שההכלה ההפוכה תמיד נכונה $A_1 \cap A_2 = A_1A_2$. אם $n > 2$ נסמן $B = \prod_{i=1}^{n-1} A_i$. לכל $i < n$ יש $x_i \in A_i, y_i \in A_n$ כך ש-$x_i + y_i = 1$. נסמן $x = \prod x_i = \prod(1 - y_i)$. מאחר ש-$1 - y_i - 1 \in A_n$ נקבל ש-$x - 1 \in A_n$. בנוסף $x \in B$ כי $x_i \in A_i$, לכן $1 \in A_n + B$ כלומר $A_n + B = R$. מכאן לפי ההנחה ש-

$$\prod_{i=1}^{n} A_i = BA_n = B \cap A_n = \bigcap_{i=1}^{n-1} A_i \cap A_n = \bigcap_{i=1}^{n} A_i$$

.

3. הגרעין של ϕ הוא $\bigcap A_i = \prod A_i$, ומאחר ש-ϕ על $R/\prod A_i \cong \bigtimes R/A_i$.

□

טענה 1.1.11. *נניח ש-$1, \beta, \ldots, \beta^{n-1} \in L$ בת"ל מעל K ויהי f הפ"מ של β. אם L/K ספרבילית אז $\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N(f'(\beta))$.*

הוכחה. המטריצה

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ \beta^{(1)} & \beta^{(2)} & \ldots & \beta^{(n)} \\ \vdots & \vdots & \ldots & \vdots \\ {\beta^{(1)}}^{n-1} & {\beta^{(2)}}^{n-1} & \ldots & {\beta^{(n)}}^{n-1} \end{pmatrix}$$

היא מטריצת ונדרמונד (Vandermonde) , לכן הדטרמיננטה שלה היא $\prod_{i<j}(\beta^{(j)} - \beta^{(i)})$. לפי טענה 1.1.9 הדיסקרימיננטה היא

$$(\prod_{i<j}(\beta^{(j)} - \beta^{(i)}))^2 = \prod_{i<j}(\beta^{(j)} - \beta^{(i)})(-1)^{n(n-1)/2}\prod_{j<i}(\beta^{(i)} - \beta^{(j)}) =$$

$$= (-1)^{n(n-1)/2}\prod_{i\neq j}(\beta^{(j)} - \beta^{(i)})$$

כעת $f(x) = \prod(x - \beta^{(i)})$ לכן $(f'(\beta))^{(j)} = f'(\beta^{(j)}) = \prod_{i,i\neq j}(\beta^{(j)} - \beta^{(i)})$. מכאן ש-

$$N(f'(\beta)) = \prod_{j}\prod_{i,i\neq j}(\beta^{(j)} - \beta^{(i)}) = \prod_{i\neq j}(\beta^{(j)} - \beta^{(i)})$$

ומכאן התוצאה.

□

1.2 פריקות יחידה בשדות מספרים אלגבריים

הגדרה 1.2.1. *תת שדה $F \subset \mathbb{C}$ נקרא שדה מספרים אלגבריים אם הוא הרחבה סופית של $\mathbb{Q}$.*

מעתה F יציין שדה מספרים אלגבריים. נעיר שכל $a \in F$ הוא אכן מספר אלגברי, מכיוון שהרחבה סופית היא אלגברית. מאותה סיבה $F/\mathbb{Q}$ ספרבילית.

הגדרה 1.2.2. *$a \in \mathbb{C}$ נקרא שלם אלגברי אם קיים פולינום מתוקן $p \in \mathbb{Z}[x]$ ש-a שורש שלו.*

קבוצה W של מספרים מרוכבים תיקרא מודול מעל השלמים אם היא סגורה לחיבור ולחיסור ואם קיימים מספרים מרוכבים $\gamma_1, \ldots, \gamma_l$ כך שכל $\gamma \in W$ הוא מהצורה $\sum b_i\gamma_i$ עם $b_i \in \mathbb{Z}$.
נוכיח שקבוצת השלמים האלגבריים היא חוג באופן דומה להוכחה המוכרת שקבוצת המספרים האלגבריים היא שדה. אם ω מספר מרוכב כך ש-$\omega\gamma \in W$ לכל $\gamma \in W$ אז $\omega\gamma_i \in W$ לכל i, לכן

$$\omega\gamma_i = \sum_j a_{ij}\gamma_j, a_{ij} \in \mathbb{Z}$$

מכאן ש-$\sum_j (a_{ij} - \delta_{ij}\omega)\gamma_j = 0$, כלומר ה-$\gamma_j$ הם מקדמים של צירוף לינארי מתאפס של עמודות המטריצה $(a_{ij} - \delta_{ij}\omega)$ לכן הדטרמיננטה שלה היא 0. פיתוח של הדטרמיננטה נותן ש-ω מאפס פולינום מתוקן ממעלה l עם מקדמים שלמים, כלומר הוא שלם אלגברי.
כעת אם a_1, a_2 שלמים אלגבריים נרשום $a_1^n + \cdots + r_n = 0, a_2^m + \cdots + s_m = 0$ עם r_i, s_i שלמים. יהי W המודול מעל השלמים שמתקבל מכל הצירופים הלינאריים בשלמים של $a_1^ia_2^j, 0 \leq i < n, 0 \leq j < m$. עבור $\gamma \in W$ מתקיים $a_1\gamma, a_2\gamma \in W$ מאחר ש

$$a_1 \sum_{0 \leq i < n, 0 \leq j < m} b_{ij}a_1^ia_2^j = \sum b_{ij}a_1^{i+1}a_2^j = \sum_{1 \leq i < n+1, 0 \leq j < m} b_{i-1,j}a_1^ia_2^j =$$

$$= \sum_{1 \leq i < n, 0 \leq j < m} b_{i-1,j}a_1^ia_2^j + \sum_{0 \leq j < m} b_{n-1,j}a_1^na_2^j$$

כעת $a_1^n = -r_1a_1^{n-1} - \cdots - r_n$ כלומר המחובר השני שווה ל

$$\sum_{0 \leq j < m} b_{n-1,j}(-r_1a_1^{n-1} - \cdots - r_n)a_2^j$$

שהוא צירוף בשלמים של $a_1^ia_2^j, 0 \leq i < n, 0 \leq j < m$. מאחר שגם המחובר הראשון הוא צירוף כזה נקבל ש-$a_1\gamma \in W$, ובאותו אופן $a_2\gamma \in W$. מכאן שגם $(a_1 + a_2)\gamma, (a_1a_2)\gamma \in W$ ולכן שניהם שלמים אלגבריים, כלומר השלמים האלגבריים אכן מהווים חוג.
בנוסף, רציונלי שהוא שלם אלגברי הוא שלם, לפי הלמה של גאוס.

הגדרה 1.2.3. *תת הקבוצה D של F שמורכבת מהשלמים האלגבריים נקראת חוג השלמים האלגבריים ב-F.*

זה אכן חוג, בתור החיתוך של F עם חוג השלמים האלגבריים.
באופן כללי D אינו תפ"י, אבל הוא כן חוג דדקינד, כלומר כל אידאל שונה מ-0 ניתן לכתיבה באופן יחיד כמכפלת אידאליים ראשוניים. יתרת הסעיף תוקדש להוכחה של העובדה הזו.
בהמשך כשנרשום אידאל נתכוון לאידאל שונה מ-0.

למה 1.2.4. *יהי $\beta \in F$. אז יש $0 \neq b \in \mathbb{Z}$ כך ש-$b\beta \in D$.*

הוכחה. קיימים $\frac{a_i}{b_i} \in \mathbb{Q}$ כך ש-a_i, b_i שלמים, $\frac{a_n}{b_n} \neq 0$ ו

$$\sum \frac{a_i}{b_i}\beta^i = 0$$

נכפול ב-$\prod b_i$ ונקבל ש

$$\sum c_i\beta^i = 0$$

כאשר $c_i = a_i \prod_{j\neq i} b_j \in \mathbb{Z}$. נכפול ב-$c_n^{n-1}$ ונקבל

$$(c_n\beta)^n + \sum c_n^{n-1-i}c_i(c_n\beta)^i = 0$$

כלומר $c_n\beta \in D$ כי הוא מאפס פולינום מתוקן במקדמים שלמים. $\square$

טענה 1.2.5. *כל אידאל $A \lhd D$ מכיל בסיס של $F/\mathbb{Q}$.*

הוכחה. יהי (β_i) בסיס להרחבה. לפי למה 1.2.4 יש (b_i) שלמים שונים מ-0 כך ש-$b_i\beta_i \in D$, לכן עבור $b = \prod b_i \neq 0$ מתקיים $b\beta_i \in D$.
יהי $0 \neq \alpha \in A$. מכיוון ש-A אידאל $b\beta_i\alpha \in A$. אם $q_i \in \mathbb{Q}$ מקיימים

$$b\alpha \sum q_i\beta_i = \sum q_i b\beta_i\alpha = 0$$

אז $\sum q_i\beta_i = 0$ ולכן $q_i = 0$, כלומר $(b\beta_i\alpha)$ בת"ל ולכן בסיס. $\square$

בהמשך הסעיף נתייחס לנורמה, עקבה ודיסקרימיננטה ביחס ל-$F/\mathbb{Q}$.

טענה 1.2.6. *אם $\alpha \in D$ אז $N(\alpha), t(\alpha) \in \mathbb{Z}$.*

הוכחה. יהי $p \in \mathbb{Z}[x]$ מתוקן כך ש-$p(\alpha) = 0$. המונומורפיזמים σ_i שומרים על $\mathbb{Q}$ ולכן גם על $\mathbb{Z}$, לכן $p(\alpha^{(i)}) = 0$. מכאן שהצמודים של α הם שלמים אלגבריים, ולכן גם הנורמה והעקבה של α שלמים אלגבריים (כמכפלה וסכום של כאלה). בנוסף הנורמה והעקבה רציונליות, ולכן הן שלמות. $\square$

מכיוון שהעקבה שלמה, גם הדיסקרימיננטה של n איברים מ-D שלמה, בתור דטרמיננטה של מטריצה של איברים שלמים.

טענה 1.2.7. *יהי A אידאל ב-D ויהי $(\alpha_i) \subset A$ בסיס של $F/\mathbb{Q}$ עבורו $|\Delta((\alpha_i))|$ מינימלי. אז כל איבר ב-A הוא צירוף לינארי בשלמים של (α_i).*

נסמן ב-$[x]$ את החלק השלם של x וב-$\langle x\rangle$ את החלק השברי שלו.

הוכחה. יהי $\alpha \in A$. אז יש $\gamma_i \in \mathbb{Q}$ כך ש $\alpha = \sum \gamma_i \alpha_i$. נניח שיש $\gamma_i \notin \mathbb{Z}$ ונראה שקיים בסיס שהערך המוחלט של הדיסקרימיננטה שלו קטן יותר. בה"כ נניח שזה γ_1. נסמן

$$\beta_1 = \alpha - [\gamma_1]\alpha_1, \beta_2 = \alpha_2, \dots, \beta_n = \alpha_n$$

אז $\beta_i \in A$ ($\beta_1 \in A$ כי A אידאל). אם

$$\sum q_i \beta_i = 0$$

אז

$$q_1(\langle\gamma_1\rangle\alpha_1 + \sum_{i\geq 2}\gamma_i\alpha_i) + \sum_{i\geq 2} q_i\alpha_i = 0$$

לכן

$$q_1\langle\gamma_1\rangle\alpha_1 + \sum_{i\geq 2}(q_1\gamma_i + q_i)\alpha_i = 0$$

ולכן

$$q_1\langle\gamma_1\rangle = 0, q_1\gamma_i + q_i = 0$$

γ_1 לא שלם לכן $\langle\gamma_1\rangle \neq 0$, לכן $q_1 = 0$ ולכן לכל $i \geq 2$ גם $q_i = 0$, כלומר (β_i) בת"ל ולכן בסיס.
המטריצה של ההעתקה $T(\alpha_i) = \beta_i$ לפי (α_i) היא

$$\begin{pmatrix} \langle\gamma_1\rangle & 0 \\ \gamma & I \end{pmatrix}$$

כאשר 0 וקטור שורה שמורכב מ-$n-1$ אפסים, $\gamma = (\gamma_i)^t_{i\geq 2}$ ו-I מטריצת היחידה מסדר $n-1$. ע"י פיתוח לפי שורה ראשונה וטענה 1.1.8 נקבל

$$|\Delta((\beta_i))| = \langle\gamma_1\rangle^2|\Delta((\alpha_i))| < |\Delta((\alpha_i))|$$

בסתירה למינמליות $|\Delta((\alpha_i))|$.
לכן $\gamma_i \in \mathbb{Z}$, כלומר α צ"ל בשלמים של (α_i). □

תמיד קיים בסיס שערכה המוחלט של הדיסקרימיננטה שלו מינימלי, כי כפי שהראינו זה מספר שלם חיובי.

הגדרה 1.2.8. *בסיס (α_i) הוא בסיס שלם של אידאל A ב-D אם כל איבר ב-A הוא צ"ל בשלמים של (α_i).*

לפי טענה 1.2.8 וההערה אחריה לכל אידאל קיים בסיס שלם.
אם $(\alpha_i), (\beta_i)$ בסיסים שלמים של אידאל A אז האיברים במטריצה המייצגת לפי (α_i) של $T(\alpha_i) = \beta_i$ שלמים, וגם האיברים במטריצה המייצגת לפי (β_i) של $S(\beta_i) = \alpha_i$ שלמים. לכן $\det T$ שלמה וגם $\det S = \det T^{-1} = \frac{1}{\det T}$ שלמה, ולכן $(\det T)^2 = 1$. לפי טענה 1.1.8 הדיסקרימיננטה של שני הבסיסים שווה, מה שמוביל להגדרה הבאה.

הגדרה 1.2.9. *יהי $A \lhd D$ אידאל. הדיסקרימיננטה של A, שנסמן ב-ΔA, היא הדיסקרימיננטה של בסיס שלם כלשהו של A.*
הדיסקרימיננטה δ_F של $F/\mathbb{Q}$ היא ΔD.

למה 1.2.10. *אם A אידאל ב-D אז* $A \cap \mathbb{Z} \neq 0$.

הוכחה. יהי $0 \neq \alpha \in A$. קיימים $a_i \in \mathbb{Z}$ כך ש-$\alpha^m + \cdots + a_0 = 0$. אם $a_0 = 0$ ו- i_0 הוא האינדקס המינימלי עבורו $a_{i_0} \neq 0$ אז נחלק את המשוואה ב-α^{i_0} ונקבל משוואה מאותה צורה שבה האיבר החופשי בפולינום שונה מ-0. לכן נוכל להניח ש-$a_0 \neq 0$, ולכן (כאשר $a_m = 1$)

$$a_0 = -\alpha \sum_{i \geq 1} a_i \alpha^{i-1} \in A$$

כלומר $0 \neq a_0 \in \mathbb{Z} \cap A$. □

טענה 1.2.11. *לכל אידאל A ב-D המנה D/A סופית.*

הוכחה. לפי למה 1.2.11 יש $0 \neq a \in \mathbb{Z} \cap A$. ההעתקה $D/(a) \to D/A$, $x + (a) \mapsto x + A$ מוגדרת היטב (אם $x - y \in (a)$ אז $x - y \in A$) ועל (מקור של $x + A$ הוא $x + (a)$), לכן מספיק להראות ש-$D/(a)$ סופי.
יש בסיס שלם (α_i) של D. נגדיר

$$S = \{\sum \gamma_i a_i : 0 \leq \gamma_i < a, \gamma_i \in \mathbb{Z}\}$$

יהי $x = \sum m_i a_i \in D$, כאשר $m_i \in \mathbb{Z}$. נחלק את m_i ב-a עם שארית ונקבל $m_i = q_i a + \gamma_i, 0 \leq \gamma_i < a$. אז

$$x - \sum \gamma_i a_i = \sum q_i a a_i + \gamma_i a_i - \sum \gamma_i a_i = a \sum q_i a_i \in (a)$$

לכן $\sum \gamma_i a_i \in x + (a)$ ולכן כל מחלקה של (a) ב-D מכילה איבר מ-S. לכל $s \in S$ קיימת מחלקה יחידה $x + (a)$ שהוא נמצא בה. נגדיר $f(s) = x + (a)$. לפי מה שהראינו f על, ובגלל ש-S סופית גם $D/(a)$ סופי. נוכיח בנוסף שהיא חח"ע כדי להראות שיש בדיוק a^n איברים במנה. אם $f(\sum \gamma_i \omega_i) = f(\sum \gamma_i' \omega_i)$ אז $\sum(\gamma_i - \gamma_i' \omega_i) \in (a)$, לכן יש $\sum m_i \omega_i \in D, m_i \in \mathbb{Z}$ כך ש-$\sum(\gamma_i - \gamma_i')\omega_i = a \sum m_i \omega_i$, כלומר כך ש-$\sum(\gamma_i - \gamma_i' - a m_i)\omega_i = 0$. מאחר ש-$(\omega_i)$ בת"ל נקבל ש-$\gamma_i - \gamma_i' = a m_i$, ומאחר ש-$-a < \gamma_i - \gamma_i' < a$ בהכרח $\gamma_i = \gamma_i'$, כלומר f חח"ע ועל ולכן יש a^n איברים ב-$D/(a)$. □

טענה 1.2.12. *D נתרי, כלומר לכל סדרה עולה $A_1 \subseteq A_2 \subseteq \ldots$ של אידאלים מתקיים החל ממקום מסוים $A_i = A_{i+1}$.*

הוכחה. תהי $A_1 \subseteq A_2 \subseteq \ldots$ סדרה עולה של אידאלים. D/A_1 סופי לכן לפי משפט ההתאמה יש מספר סופי של אידאלים שמכילים את A_1, ומכאן ש-$\{A_i\}_i$ סופית, כלומר החל ממקום מסוים $A_i = A_{i+1}$. □

טענה 1.2.13. *כל אידאל ראשוני ב-D הוא מקסימלי.*

הוכחה. אם P אידאל ראשוני אז לכל $0 \neq r \in D/P$ הפונקציה $x \mapsto rx$ חח"ע מאחר ש-D/P תחום שלמות, ומאחר שהוא סופי היא גם על, ובפרט קיים x כך ש-$rx = 1$. מכאן ש-r הפיך ולכן D/P שדה, כלומר P מקסימלי. $\square$

נמשיך בטענות כדי להראות ש-D חוג דדקינד.

למה 1.2.14. *יהי A אידאל ב-D. אם $\beta \in F$, $\beta A \subset A$ אז $\beta \in D$.*

הוכחה. יש ל-A בסיס שלם (α_i). מתקיים $(\beta\alpha_i) \subset A$ לכן יש $a_{ij} \in \mathbb{Z}$ כך ש-$\beta\alpha_i = \sum_j a_{ij}\alpha_j$. לכן

$$\sum_j (a_{ij} - \delta_{ij}\beta)\alpha_j = 0$$

מכאן שצ"ל לא טריוויאלי של עמודות המטריצה $(a_{ij}) - \beta I$ מתאפס, ולכן המטריצה לא הפיכה, כלומר b שורש של הפולינום האופייני של (a_{ij}). הפ"א מתוקן וכל המקדמים שלו שלמים, לכן $\beta \in D$. $\square$

למה 1.2.15. *יהיו A, B אידאלים ב-D כך ש-$A = AB$. אז $B = D$.*

הוכחה. יש ל-A בסיס שלם (α_i). בגלל ש-$A = AB$ יש $a_{ij} \in A, b_{ij} \in B$ כך ש $\alpha_i = \sum_j a_{ij}b_{ij}$. יש c_{ijk} כך ש $a_{ij} = \sum_k c_{ijk}\alpha_k$, לכן

$$\alpha_i = \sum_j b_{ij} \sum_k c_{ijk}\alpha_k = \sum_j \sum_k b_{ij}c_{ijk}\alpha_k = \sum_k (\sum_j b_{ij}c_{ijk})\alpha_k$$

נסמן $d_{ik} = \sum_j b_{ij}c_{ijk}$ ונקבל ש $\alpha_i = \sum_k d_{ik}\alpha_k$ ו-$d_{ik} \in B$ כי B אידאל. לכן

$$\sum_k (d_{ik} - \delta_{ik})\alpha_k = 0$$

ולכן צ"ל לא טריוויאלי של עמודות המטריצה $(d_{ik}) - I$ מתאפס. מכאן שהיא לא הפיכה, ולכן 1 מאפס את הפ"א של (d_{ik}). הפ"א מתוקן וכל המקדמים למעט העליון הם פולינומים באיברי A, כלומר יש $\beta_i \in B$ כך ש-$0 = 1 + \sum \beta_i$ ולכן $1 = -\sum \beta_i \in B$. מכאן ש-$B = D$. $\square$

טענה 1.2.16. *אם A, B אידאלים ב-D ו-$\omega \in D$ מקיים $BA = (\omega)A$ אז $B = (\omega)$.*

הוכחה. אם $\beta \in B$ אז $(\frac{\beta}{\omega})A \subset A$, כי לכל $a \in A$ קיים $a' \in A$ כך ש-$\beta a = \omega a'$ ולכן $\frac{\beta}{\omega}a = a' \in A$. לפי למה 1.2.14 $\frac{\beta}{\omega} \in D$, ומכאן ש $\frac{B}{\omega} = \{\frac{\beta}{\omega} : \beta \in B\} \subset D$ אידאל. מתקיים $A = A\frac{B}{\omega}$ כי לכל $\alpha \in A, \beta \in B$ מתקיים $\frac{\beta}{\omega} \in D$ ולכן $\alpha\frac{\beta}{\omega} \in A$, ו $\alpha = \alpha'\frac{\beta}{\omega}$ עבור α', β כך ש-$\omega\alpha = \alpha'\beta$.

לפי למה 1.2.15 מתקיים $D = \frac{B}{\omega}$, ולכן לכל $x \in D$ קיים $\beta \in B$ עבורו $x = \frac{\beta}{\omega}$, כלומר $x\omega = \beta \in B$. מכאן ש-$B = (\omega)$.

□

הגדרה 1.2.17. *נאמר ששני אידאלים A, B ב-D הם שקולים, ונסמן $A \sim B$, אם קיימים $\alpha, \beta \in D$ שונים מ-0 כך ש-$(\alpha)A = (\beta)B$. זה יחס שקילות, ומחלקות השקילות שלו נקראות מחלקות אידאלים. מספר מחלקות האידאלים h_F נקרא מספר המחלקות של F (מיד נוכיח שזה אכן מספר סופי).*

למה 1.2.18. *קיים שלם $M > 0$ כך שלכל $\alpha, \beta \in D, \beta \neq 0$ קיימים שלם $1 \le t \le M$ ו-$\omega \in D$ כך ש-$|N(t\alpha - \omega\beta)| < |N(\beta)|$.*

הוכחה. לכל $\alpha, \beta \in D, \beta \neq 0$ האי שוויון מתקיים אםם $|N(t\frac{\alpha}{\beta} - \omega)| < 1$ לכן מספיק להראות שקיים שלם $M > 0$ כך שלכל $\gamma \in F$ קיימים שלם $1 \le t \le M$ ו-$\omega \in D$ כך ש-$|N(t\gamma - \omega)| < 1$. יהי $(\omega_i)^n$ בסיס שלם ל-D. לכל $\gamma \in F$ קיימים $\gamma_i \in \mathbb{Q}$ כך ש $\gamma = \sum \gamma_i\omega_i$, לכן $g^{(j)} = \sum_i \gamma_i\omega_i^{(j)}$ ולכן

$$|N(\gamma)| = \prod_j |\sum_i \gamma_i\omega_i^{(j)}| \le \prod_j \sum_i \gamma_i|\omega_i^{(j)}| \le$$

$$\le \prod_j \sum_i \max_k \gamma_k|\omega_i^{(j)}| = \max_k \gamma_k \prod_j \sum_i |\omega_i^{(j)}|$$

נסמן $C = \prod_j \sum_i |\omega_i^{(j)}|$ ו-$m = [C] + 1, M = m^n$. נגדיר, לכל $\gamma \in F$,

$$a_\gamma = \sum[\gamma_i]\omega_i \in D, b_\gamma = \sum\langle\gamma_i\rangle\omega_i$$

אז $\gamma = a_\gamma + b_\gamma$. נביט בהעתקה הלינארית והחח"ע $\varphi : F \to \mathbb{R}^n, \sum\gamma_i\omega_i \mapsto (\gamma_i)$. אז לכל $\gamma \in F$ מתקיים $\varphi(b_\gamma) \in [0,1]^n$. נגדיר קוביות

$$C_{k_1,\dots,k_n} = \bigtimes[\frac{k_i}{m}, \frac{k_i+1}{m}]$$

עבור k_i שלמים בין 0 ל-$m-1$. יש $M = m^n$ קוביות כאלה. תהי $\gamma \in F$. לפי עקרון שובך היונים שתיים מהנקודות $(\varphi(b_{k\gamma}))_{k=1}^{M+1}$ נמצאות באותה קוביה מהאוסף $(C_{(k_i)})$. נסמן שתיים כאלה ב-$\varphi(b_{h\gamma}), \varphi(b_{l\gamma})$. אז $(h-l)\gamma = a_{h\gamma} + b_{h\gamma} - a_{l\gamma} - b_{l\gamma} = \omega + \delta$, כאשר $\omega = a_{h\gamma} - a_{l\gamma} \in D$ ו-$\delta = b_{h\gamma} - b_{l\gamma}$. נרשום $\delta = \sum\delta_i\omega_i$. מתקיים $(\delta_i) = \varphi(\delta) = \varphi(b_{h\gamma}) - \varphi(b_{l\gamma})$ והקואורדינטה ה-i של כל מחובר באגף ימין היא ב-$[\frac{k_i}{m}, \frac{k_i+1}{m}]$ לכן ההפרש שלהן ב-$[0, \frac{1}{m}]$, כלומר $\delta_i \in [0, \frac{1}{m}]$ ולכן

$$|N(t\gamma - \omega)| = |N(\delta)| \le \frac{C}{m^n} < 1$$

□

משפט 1.2.19. *מספר המחלקות של F סופי.*

הוכחה. יהי M מהלמה הקודמת. לפי טענה 1.2.11 ולפי משפט ההתאמה יש מספר סופי של אידאלים שמכילים את $(M!)$, ולכן יש מספר סופי של אידאלים שמכילים את $M!$. יהי A אידאל ב-D. לפי טענה 1.2.6, הערך המוחלט של הנורמה של כל $0 \neq \alpha \in A$ הוא מספר שלם חיובי, לכן יש $0 \neq \beta \in A$ כך ש-$|N(\beta)|$ מינימלי. לכל $\alpha \in A$ יש $1 \leq t \leq M$ ו-$\omega \in D$ כך ש-$|N(t\alpha - \omega\beta)| < |N(\beta)|$. A אידאל לכן $t\alpha - \omega\beta \in A$, ולכן $t\alpha - \omega\beta = 0$. כלומר, $t\alpha \in (\beta)$, ולכן $M!\alpha \in (\beta)$, כלומר $M!A \subset (\beta)$. נסמן $B = \frac{1}{\beta}M!A$. לכל $\frac{1}{\beta}M!\alpha \in B$ מתקיים $M!\alpha \in (\beta)$ ולכן $\frac{1}{\beta}M!\alpha \in D$, כלומר $B \subset D$. B אידאל ו- $M!A = (\beta)B$, ולכן בגלל ש-$\beta \in A$ מתקיים $M!\beta \in (\beta)B$, כלומר $M! \in B$. מאחר ש-$(\beta)B = (M!)A$ האידאלים A ו-B שקולים, כלומר כל אידאל שקול לאחד מהמספר הסופי של האידאלים שמכילים את $M!$, ולכן מספר המחלקות של F סופי. $\square$

טענה 1.2.20. *יהי A אידאל ב-D. אז יש $1 \leq k \leq h_F$ כך ש-A^k ראשי.*

הוכחה. לפי עקרון שובך היונים קיימים $1 \leq i < j \leq h_F + 1$ כך ש-A^i, A^j נמצאים באותה מחלקת אידאלים. לכן יש $\alpha, \beta \in D$ כך ש-$(\beta)A^j = (\alpha)A^i$. נסמן $k = j - i$. מתקיים $\frac{\alpha}{\beta}A^i \subset A^j \subset A^i$, לכן לפי למה 1.2.14, $\frac{\alpha}{\beta} \in D$. מאחר ש-$A^kA^i = A^j = (\frac{\alpha}{\beta})A^i$ נקבל מטענה 1.2.16 ש-$A^k = (\frac{\alpha}{\beta})$. $\square$

טענה 1.2.21. *אם A, B, C אידאלים ב-D עבורם $AB = AC$ אז $B = C$.*

הוכחה. יש k כך ש-A^k ראשי. מתקיים $A^kB = A^kC$ ולכן $B = C$. $\square$

טענה 1.2.22. *אם $A \subset B$ אידאלים אז יש אידאל C כך ש-$A = BC$.*

הוכחה. יש k ו-$\beta \in D$ כך ש-$B^k = (\beta)$. מכיוון ש-$A \subset B$ מתקיים $B^{k-1}A \subset B^k = (\beta)$ ולכן $(\frac{1}{\beta})B^{k-1}A \subset D$. נסמן את הקבוצה הזו ב-$C$, אז C אידאל ו

$$BC = (\frac{1}{\beta})(\beta)A = A$$

$\square$

טענה 1.2.23. *יהי $D \neq A$ אידאל ב-D, אז A הוא הוא מכפלה של אידאלים ראשוניים.*

הוכחה. יהי P_1 אידאל מקסימלי שמכיל את A. לפי הטענה האחרונה קיים אידאל B_1 כך ש-$A = P_1B_1$. אם $D = B_1$ אז $A = P_1$ וסיימנו. אחרת אם $B_1 \neq D$ אז B_1 מוכל באידאל מקסימלי P_2 ולכן $A = P_1P_2B_2$. אם $B_2 = D$ סיימנו, אחרת נמשיך באותו אופן. אם לכל i מתקיים $B_i \neq D$ אז לכל i מתקיים $B_i = P_{i+1}B_{i+1}$ ומכאן ש-$B_i \subset B_{i+1}$. מכיוון ש-D נתרי החל ממקום מסוים $B_i = B_{i+1}$, אבל גם $DB_i = P_{i+1}B_{i+1}$, ולכן לפי טענה 1.2.21 $D = P_{i+1}$, בסתירה למקסימליות של P_{i+1}. מכאן שהחל מ-i מסוים מתקיים $B_i = D$ ולכן $A = \prod^i P_j$. □

הגדרה 1.2.24. *יהי P אידאל ראשוני ו-A אידאל. $\mathrm{ord}_P A$ מוגדר כשלם האי שלילי t המקסימלי עבורו $A \subset P^t$.*

הקיום של t כזה נובע מכך ש-$\bigcap_{n=1}^{\infty} P^n = 0$. לפי טענה 1.2.20 קיים m כך ש-P^m ראשי. מספיק להראות ש-$\bigcap_{n=1}^{\infty} P^{mn} = 0$. נרשום $P^m = (b)$ ונקבל שצריך להוכיח ש-$\bigcap_{n=1}^{\infty}(b^n) = 0$. אכן אם $x \in (b^n)$ לכל n אז קיימים a_i שעבורם $x = a_ib^i$. מכאן ש-$a_i = ba_{i+1}$ ולכן $(a_1) \subset (a_2) \subset \ldots$. מאחר ש-$D$ נתרי קיים i שעבורו $(a_i) = (a_{i+1})$, לכן $a_{i+1} = la_i$ עבור $l \in D$. מכאן ש-$lba_{i+1} = a_{i+1}$, והואיל ש-b לא הפיך $a_{i+1} = 0$ ולכן גם $x = 0$ כנדרש.

טענה 1.2.25. *יהיו A, B, P, P' אידאלים ב-D ונניח ש-$P \neq P'$ ושניהם ראשוניים. אז*

1. $\mathrm{ord}_P P = 1$

2. $\mathrm{ord}_P P' = 0$

3. $\mathrm{ord}_P AB = \mathrm{ord}_P A + \mathrm{ord}_P B$

הוכחה. 1. $P \subset P$ ואם $P \subset P^2$ אז $P = PP$ ולפי למה 1.2.15 מתקיים $P = D$. זה לא ייתכן כי P ראשוני, ולכן $\mathrm{ord}_P P = 1$.

2. P' ראשוני לכן מקסימלי, ומכאן ש-$P \not\subset P'$. לכן $\mathrm{ord}_P P' = 0$.

3. נסמן $t = \mathrm{ord}_P A, s = \mathrm{ord}_P B$. לפי טענה 1.2.22 יש אידאלים A_1, B_1 כך ש-$A = P^tA_1, B = P^sB_1$. אם $A_1 = PA_2$ אז $A = P^{t+1}A_2$ ואז $A \subset P^{t+1}$, וזה לא ייתכן. לכן $A_1 \neq PA_2$ לכל אידאל A_2 ולפי טענה 1.2.22 $A_1 \not\subset P$ ובאופן דומה $B_1 \not\subset P$. מתקיים $AB = P^{s+t}A_1B_1$. אם $AB \subset P^{s+t+1}$ אז יש אידאל C כך ש

$$P^{s+t}A_1B_1 = AB = P^{s+t}PC$$

לכן $PC = A_1B_1$ לפי טענה 1.2.21. מכאן ש-$A_1B_1 \subset P$, ומאחר ש-P ראשוני $A_1 \subset P$ או $A_2 \subset P$, בסתירה למה שהראנו. מכאן ש-$P^{s+t} \subset AB, P^{s+t+1} \not\subset AB$ ולכן $\mathrm{ord}_P AB = \mathrm{ord}_P A + \mathrm{ord}_P B$. □

משפט 1.2.26. *יהי A אידאל ב-D. אז $A = \prod P^{a(P)}$ כאשר המכפלה היא על כל האידאלים הראשוניים ב-D ו-$a(P)$ הם שלמים אי שליליים שכמעט כולם 0. בנוסף, בכל רישום כזה $a(P) = \mathrm{ord}_P A$.*

הוכחה. קיימת הצגה כזו לפי טענה 1.2.23. יהי P_0 אידאל ראשוני, אז לפי הטענה הקודמת

$$\mathrm{ord}_{P_0} A = \sum_P a(P) \mathrm{ord}_{P_0} P = a(P_0)$$

$\square$

טענה 1.2.27. *יהיו $A \subset B$ חוגים חילופיים עם יחידה, ונניח ש-B שלם מעל A, כלומר לכל $b \in B$ קיים פולינום מתוקן $p \in A[x]$ ש-b שורש שלו. יהי $P \subset A$ אידאל ראשוני. אז קיים אידאל ראשוני $Q \subset B$ כך ש-$P = Q \cap A$.*

הוכחת הטענה חורגת מהעבודה,ז אך נשתמש בה בהמשך.

1.3 הסתעפות ומעלה

לפי למה 1.2.10 לכל אידאל ראשוני P של D החיתוך $P \cap \mathbb{Z}$ אינו 0. זה אידאל ראשוני של $\mathbb{Z}$ ולכן הוא נוצר על ידי ראשוני p.
בנוסף D/P הוא שדה סופי שמכיל את $\mathbb{Z}/(\mathbb{Z} \cap P) = \mathbb{Z}/p\mathbb{Z}$, לכן קיים f כך ש-p^f הוא מספר האיברים ב-D/P.

הגדרה 1.3.1. *אינדקס ההסתעפות של P הוא $\mathrm{ord}_P(p)$, והמעלה של P היא f.*

טענה 1.3.2. *יהי P אידאל ראשוני ב-D עם מעלה f. אז מספר האיברים ב-D/P^e הוא p^{ef}.*

הוכחה. נוכיח באינדוקציה על e. הטענה נכונה עבור $e = 1$. נניח שהיא נכונה ל-$e > 1$, $e-1$.
יש תת חבורה של D/P^e שאיזומורפית ל-P^{e-1}/P^e, ולפי משפט האיזומורפיזם השני

$$(D/P^e)/(P^{e-1}/P^e) \cong D/P^{e-1}$$

אם נראה שב-P^{e-1}/P^e יש p^f איברים אז ב-D/P^e יהיו $p^f \cdot p^{(e-1)f} = p^{ef}$ איברים כנדרש.
אם $P^e = P^{e-1}$ אז $P = D$ וזה לא ייתכן כי P ראשוני, לכן יש $\alpha \in P^{e-1} - P^e$. מאחר ש-$P^e \subset (a) + P^e$ קיים אידאל A כך ש $A((a) + P^e) = P^e$. יהי Q גורם בהצגה של $(a) + P^e$ כמכפלת ראשוניים שהחזקה שלו שונה מ-0. אז (אם נסמן ב-B את מכפלת הגורמים בהצגה עם Q בחזקה מופחתת ב1)

$$AQB = P^e$$

כלומר, $P^e \subset Q$ ולכן $P \subset Q$, כלומר $P = Q$ כי P מקסימלי. מכאן שכל הגורמים בהצגה של $(a) + P^e$ הם P, כלומר יש n כך שהאידאל שווה ל-P^n. מתקיים $P^n = (a) + P^e \subset P^{e-1}$.
אם $n < e-1$ אז $P^n = P^{e-1-n}P^n$ ולכן $P^{e-1-n} = D$, בסתירה לכך שהוא מוכל ממש ב-P^{e-n} (אחרת $P^{e-1-n} = P^{e-1-n}P$ כלומר $P = D$ וזה לא ייתכן). אם $n > e-1$ אז $P^n = P^e$ וזה לא ייתכן כי $\alpha \in P^n, a \notin P^e$. מכאן ש-$n = e-1$. יהי $f : D \to P^{e-1}/P^e$ האפימורפיזם $f(\gamma) = \gamma\alpha + P^e$. איבר γ בגרעין אםם $(\gamma\alpha) \subset P^e$ אםם $\mathrm{ord}_P(\gamma\alpha) \geq e$. מאחר ש-$\mathrm{ord}_P(\gamma\alpha) = \mathrm{ord}_P(\gamma) + e - 1$ האיבר γ הוא בגרעין אםם $\mathrm{ord}_P(\gamma) \geq 1$, כלומר אםם $\gamma \in P$.
לפי משפט האיזומורפיזם הראשון $D/P \cong P^{e-1}/P^e$ כנדרש. $\square$

משפט 1.3.3. *יהי p ראשוני ויהיו $(P_i)^g$ האידאלים הראשוניים ב-D שמכילים אותו. יהיו e_i, f_i אינדקס ההסתעפות והמעלה של P_i. אז $\sum e_i f_i = n$.*

הוכחה. לפי משפט 1.2.26 $(p) = \prod P_i^{e_i}$. עבור $i \neq j$ האידאל $P_i + P_j$ מכיל ממש את P_i המקסימלי, ולכן שווה ל-D. אם $P_i^{e_i} + P_j^{e_j} \neq D$ אז קיים אידאל מקסימלי A שמכיל את $P_i^{e_i} + P_j^{e_j}$, ומכאן שגם את $P_i^{e_i}, P_j^{e_j}$. מאחר שהוא ראשוני הוא מכיל את P_i, P_j ולכן גם את $P_i + P_j = D$, וזה לא ייתכן.
לפי טענה 1.1.10 $D/(p) \cong \bigtimes D/P^{e_i}$. מהוכחת טענה 1.2.11 נובע ש-p^n הוא מספר האיברים ב-$D/(p)$. לפי טענה 1.3.2 יש ב-$D/P_i^{e_i}$ $p^{e_i f_i}$ איברים. לכן $p^n = \prod p^{e_i f_i}$, ולכן $n = \sum e_i f_i$. $\square$

נניח ש-$F/\mathbb{Q}$ נורמלית ותהי $G = G(F/\mathbb{Q})$. אם A אידאל ו-$\sigma \in G$ אז $\sigma A = {\sigma^{-1}}^{-1}(A)$ אידאל.
לכן $D/A \cong \sigma D/\sigma A = D/\sigma A$ לפי משפט ההתאמה. בפרט אם P ראשוני אז גם σP ראשוני.

טענה 1.3.4. *יהי p ראשוני ויהיו P_i, P_j אידאלים ראשוניים ב-D שמכילים אותו. אז יש $\sigma \in G$ כך ש-$P_j = \sigma P_i$.*

הוכחה. נניח שאין σ כזה. לפי טענה 1.1.10 יש $a \in D$ כך ש-$a \in \sigma P_i, a - 1 \in P_j$. לכן $\alpha = a - 1$ מקיים $\alpha \in P_j, \alpha \notin \sigma P_i$. מכאן ש-$N(\alpha) = \prod_{\sigma\in G} \sigma\alpha \in P_j$ מאחר ש-$\alpha = \mathrm{id}\alpha$ משתתף במכפלה. בנוסף $N(\alpha)$ שלם, כלומר $N(\alpha) \in P_j \cap \mathbb{Z} = (p)$. לכן $N(\alpha) \in P_i$, ובגלל ש-P_i ראשוני יש σ עבורו $\sigma\alpha \in P_i$. אבל אז $\alpha \in \sigma^{-1}P_i$, וזה לא ייתכן. □

משפט 1.3.5. *נניח ש-$F/\mathbb{Q}$ נורמלית. יהי p ראשוני, יהיו $(P_i)^g$ האידאלים הראשוניים שמכילים אותו ויהיו e_i, f_i אינדקס ההסתעפות והמעלה של P_i. אז כל ה-e_i שווים זה לזה וכל ה-f_i שווים זה לזה. אם נסמן את הערכים המשותפים ב-e וב-f אז $efg = n$.*

הוכחה. לכל i יש σ כך ש-$P_i = \sigma P_1$. מאחר ש-$D/P_i = D/\sigma P_1 \cong D/P_1$ נקבל $f_i = f_1$, ולכן כל ה-f_i שווים זה לזה. לפי משפט 1.2.26 מתקיים $(p) = \prod P_i^{e_i}$, לכן $(p) = \prod (\sigma P_i)^{e_i}$. המעריך של $P_i = \sigma P_1$ הוא e_1, ומצד שני בהצגה המקורית הוא e_i, לכן לפי משפט 1.2.26 $e_i = e_1$ ולכן כל ה-e_i שווים זה לזה. מאחר ש-$n = \sum e_i f_i$ לפי משפט 1.3.3 נקבל ש-$n = efg$. □

2 שדות ריבועיים וציקלוטומיים

2.1 שדות מספרים ריבועיים

הגדרה 2.1.1. *שדה מספרים אלגבריים F יקרא שדה מספרים ריבועי אם* $[F:\mathbb{Q}]=2$.

בהמשך הסעיף נסמן ב-F שדה מספרים ריבועי וב-D את חוג השלמים האלגבריים שלו.

טענה 2.1.2. *קיים שלם d חופשי מריבועים כך ש-*$F=\mathbb{Q}(\sqrt{d})$.

הוכחה. נרשום $F=\mathbb{Q}(\alpha)$. α מדרגה 2 לכן יש $a,b,c\in\mathbb{Z}$ כך ש-$ax^2+bx+c=0$. לכן $a=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. נסמן $A=b^2-4ac$. אז $F=\mathbb{Q}(\sqrt{A})$. נרשום $A=A_1^2A_2$ עבור A_1,A_2 שלמים כך ש-A_2 חופשי מריבועים. אז $\sqrt{A}=A_1\sqrt{A_2}$ לכן $F=\mathbb{Q}(\sqrt{A_2})$. □

$F/\mathbb{Q}$ נורמלית בתור ש"פ של הפ"מ של d. יש ב-$G=G(F,\mathbb{Q})$ שני אוטומורפיזמים, הזהות ואוטומורפיזם שמעביר את השורש $\sqrt{d}$ של x^2-d לשורש $-\sqrt{d}$ של אותו פולינום. נסמן את האוטומורפיזם הזה ב-σ, אז לכל $\alpha=r+s\sqrt{d}\in F$ מתקיים

$$N(\alpha)=\alpha\sigma\alpha=r^2-ds^2, t(\alpha)=\alpha+\sigma\alpha=2r$$

אם העקבה והנורמה של α שלמים אז $x^2-t(\alpha)x+N(\alpha)=(x-\alpha)(x-\sigma\alpha)$ פולינום במקדמים שלמים ש-α מאפס, לכן $\alpha\in D$ אםם העקבה והנורמה שלו שלמים.

טענה 2.1.3. *אם* $d=2,3\mod 4$ *אז* $D=\{a+b\sqrt{d}:a,b\in\mathbb{Z}\}$, *אחרת* $D=\{2a+b(-1+\sqrt{d}):2a,2b\in\mathbb{Z}\}$.

הוכחה. יהי $\gamma=r+s\sqrt{d}\in F$. אז $\gamma\in D$ אםם הנורמה והעקבה שלו שלמים אםם $2r,r^2-s^2d\in\mathbb{Z}$. זה שקול לכך ש-$2r\in\mathbb{Z}$ ו $-4(r^2-s^2d)+(2r)^2=4s^2d\in\mathbb{Z}$. נרשום $2s=p/q$, כאשר p,q זרים. השייכות האחרונה שקולה לכך ש-q^2 מחלק את p^2d. מאחר ש-q^2,p^2 זרים (אם ראשוני m מחלק את p^2 אז הוא מחלק את p, לכן לא מחלק את q ולכן גם לא את q^2) זה שקול ל-$p^2|d$, כלומר (משום ש-d חופשי מריבועים) ל-$p=\pm1$ ולכך ש-$2s$ שלם.

כעת נניח ש-$\gamma\in D$ ונרשום $2r=m,2s=n$. אם $\gamma\in D$ אז $m^2-dn^2=4r^2-4s^2d=4(r^2-s^2d)$ מתחלק ב4.

אם $d=2,3\mod 4$ אז $m^2-dn^2=m^2+2n^2\mod 4$ או $m^2-dn^2=m^2+n^2\mod 4$. משום שריבוע שלם שקול ל-0 או ל-1 מודולו 4 נקבל ש-m,n שניהם זוגיים, כלומר r,s שלמים. ההכלה השנייה נובעת מכך שלכל $r,s\in\mathbb{Z}$ גם $r^2-s^2d,2r\in\mathbb{Z}$.

אחרת, $d=1\mod 4$ (הוא לא מתחלק ב4 כי הוא חופשי מריבועים). במקרה זה $m^2-dn^2=m^2-n^2\mod 4$ ולכן יש ל-m,n אותה זוגיות, כלומר $D=\{\frac{m+n\sqrt{d}}{2}:m=n\mod 2\}$ (כל איבר מהצורה הזו הוא ב-D כי $(m/2)^2-(n/2)^2d=(m^2-n^2d)/4$ שלם מאחר ש-$m^2-n^2d=m^2-n^2=0\mod 4$ ו $2(m/2)=m\in\mathbb{Z}$).

מתקיים $\frac{m+n\sqrt{d}}{2}=\frac{m+n}{2}+n\frac{-1+\sqrt{d}}{2}$, ומשום ש-$m=n\mod 2$ מתקיים $\frac{m+n}{2}\in\mathbb{Z}$. מכאן ש-$D\subset\{a+b\frac{-1+\sqrt{d}}{2}:a,b\in\mathbb{Z}\}$. את ההכלה ההפוכה נקבל מכך ש-$\frac{-1+\sqrt{d}}{2}\in D$, כי ל-$-1,1$ אותה זוגיות. □

2.2 שדות ציקלוטומיים

יהי m שלם חיובי ויהי $\zeta_m = e^{\frac{2\pi i}{m}}$. הוא יוצר של חבורת שורשי היחידה מסדר m. מאחר ש-$x^m - 1 = (x-1)(x-\zeta_m)\dots(x-\zeta_m^{m-1})$ השדה $F = \mathbb{Q}(\zeta_m)$ הוא ש"פ של $x^m - 1$, ולכן $F/\mathbb{Q}$ נורמלית. F נקרא השדה הציקלוטומי של שורשים mיים של היחידה.

כזכור מהקורס בתורת גלואה הפולינום הציקלוטומי ה-m, $\Phi_m(x) = \prod_{\gcd(a,m)=1}(x - \zeta_m^a)$, הוא בעל מקדמים שלמים ואי פריק ב-$\mathbb{Z}[x]$. מכאן שהוא הפ"מ של ζ_m. מאחר שמעלתו היא $\phi(m)$ (כאשר זו פונקציית פי של אוילר) נקבל ש-$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$.

טענה 2.2.1. *תהי $G = G(F, \mathbb{Q})$ ותהי U_m חבורת ההפיכים של $\mathbb{Z}/(m)$. יש איזומורפיזם $\theta : G \to U_m$ כך שלכל $\sigma \in G$ מתקיים $\sigma\zeta_m = \zeta_m^{\theta(\sigma)}$.*

הוכחה. מאחר ש-$\zeta_m^m = 1$ מתקיים $(\sigma\zeta_m)^m = 1$. לכן קיים ויחיד $\theta(\sigma) \in \mathbb{Z}/(m)$ כך ש-$\sigma\zeta_m = \zeta_m^{\theta(\sigma)}$. לכל σ, τ מתקיים

$$\zeta_m^{\theta(\tau\sigma)} = \tau\sigma\zeta_m = \tau(\zeta_m^{\theta(\sigma)}) = \zeta_m^{\theta(\tau)\theta(\sigma)}$$

לכן $\theta(\tau\sigma) = \theta(\tau)\theta(\sigma)$. בפרט $\theta(\sigma)\theta(\sigma^{-1}) = \theta(\mathrm{id}) = 1$, ולכן אפשר לראות את הטווח של θ כ-U_m. לפי מה שהראינו θ הומומורפיזם. אם $\theta(\sigma) = 1$ אז $\sigma\zeta_m = \zeta_m$, ולכן σ היא הזהות, כלומר θ מונומורפיזם. לבסוף, ב-G וב-U_m יש $\phi(m)$ איברים, ומכאן ש-θ איזומורפיזם. □

מעתה נרשום ζ במקום ζ_m.

משום ש-θ הפיכה, יש לה הופכית $a \mapsto \sigma_a$, שמתאימה לכל a שזר ל-m את הפונקציה σ_a שמקיימת $\sigma_a\zeta = \zeta^a$.

למה 2.2.2. *אם $(\alpha_i)_i \subset D$ בסיס ו-Δ הדיסקרימיננטה שלו אז $(\Delta) \subset \{\sum m_i\alpha_i : m_i \in \mathbb{Z}\}$.*

הוכחה. יהי $\sum r_i\alpha_i = w \in D, r_i \in \mathbb{Q}$. נכפול ב-$\alpha_j$ ונקבל ש-$t(w\alpha_j) = \sum r_i t(\alpha_i\alpha_j)$. העקבות שלמות כי האיברים שלמים אלגבריים, לכן ע"י שימוש בכלל קרמר מקבלים ש-r_i הוא מהצורה $m_i/\Delta, m_i \in \mathbb{Z}$, כלומר $\Delta w = \sum m_i\alpha_i$. □

למה 2.2.3. *הדיסקרימיננטה Δ של $(1, \zeta, \dots, \zeta^{\phi(m)-1})$ מחלקת את $m^{\phi(m)}$.*

הוכחה. ζ שורש של $x^m - 1$ לכן יש g כך ש-$x^m - 1 = \Phi_m(x)g(x)$. נגזור ונקבל $mx^{m-1} = \Phi'_m(x)g(x) + \Phi_m(x)g'(x)$. בפרט $m\zeta^{m-1} = \Phi'_m(\zeta) + g(\zeta)$. הנורמה של ζ היא 1 או -1, לכן לפי טענה 1.1.11 יש n_1, n_2 כך ש

$$(-1)^{n_1}\prod_{i=1}^{\phi(m)} m = (-1)^{n_2}\Delta g(\zeta)$$

כלומר $\Delta g(\zeta)(-1)^{n_2-n_1} = m^{\phi(m)}$ ולכן $\Delta | m^{\phi(m)}$. □

עד סוף הסעיף p יהיה ראשוני שלא מחלק את m. בגלל שהוא לא מחלק את m הם זרים, לכן קיימת σ_p.

טענה 2.2.4. *יהי p ראשוני שלא מחלק את m ויהי $w \in D$. אז יש $\sum a_i\zeta^i \in Z[\zeta]$ כך ש-$w - \sum a_i\zeta^i \in (p)$.*

הוכחה. תהי Δ הדיסקרימיננטה של $1, \zeta, \ldots, \zeta^{\phi(m)-1}$. p לא מחלק את $m^{\phi(m)}$ כי הוא ראשוני, ולפי הלמה הקודמת הוא לא מחלק את Δ. לכן יש $a, b \in \mathbb{Z}$ כך ש-$a\Delta + bp = 1$, כלומר $a\Delta - 1 \in (p)$. לכן גם $wa\Delta - w \in (p)$. החוג בלמה 2.2.2 עם $\alpha_i = \zeta^i$ הוא $Z[\zeta]$, לכן $w\Delta \in Z[\zeta]$. מכאן שגם $wa\Delta \in Z[\zeta]$ ולכן הוא איבר כנדרש. □

טענה 2.2.5. *נניח ש-p ראשוני שלא מחלק את m וש-$n > 0$ מקיים $p^n = 1 \mod m$. אז לכל $w \in D$, $w^{p^n} - w \in (p)$.*

הוכחה. לפי הטענה הקודמת $w - \sum a_i\zeta^i \in (p)$ עם $a_i \in \mathbb{Z}$. מאחר ש-$a_i^p - a_i \in (p)$ והאופיין של $D/(p)$ הוא p מתקיים $w^p - \sum a_i\zeta^{pi} \in (p)$. מכיוון ש-$(w^{p^k})^p = w^{p^{k+1}}$ אם נחזור על התהליך n פעמים נקבל ש-$w^{p^n} - \sum a_i\zeta \in (p)$, כי $\zeta^{p^n} = \zeta$. מכאן ש-

$$w^{p^n} - w = w^{p^n} - \sum a_i\zeta^i + \sum a_i\zeta^i - w \in (p)$$

□

טענה 2.2.6. *אם p ראשוני שלא מחלק את m אז אינדקס ההסתעפות של כל אידאל ראשוני P ב-D שמכיל את p הוא 1.*

הוכחה. נניח שאינדקס ההסתעפות גדול מ-1, אז $(p) \subset P^2$. יהי $w \in P - P^2$ (קיים כזה כי $P = P^2 \implies P = D$). מאחר שיש מספר סופי של מחלקות שקילות מודולו m יש $i > j$ כך ש-$p^i = p^j \mod m$, לכן עבור $n = i - j > 0$ מתקיים $p^n = 1 \mod m$. לפי הטענה הקודמת $w^{p^n} - w \in (p)$ ולכן $w^{p^n} - w \in P^2$, ומכאן ש-$w = w - w^{p^n} + w^{p^n} \in P^2$ כי $w^{p^n} \in P^2$, בסתירה לבחירת w. □

נעיר שאידאל ראשוני שאינדקס ההסתעפות שלו הוא 1 נקרא בלתי מסועף.

טענה 2.2.7. *לכל $w \in D$ מתקיים $\sigma_p w - w^p \in (p)$.*

הוכחה. לפי טענה 2.2.4 יש a_i שלמים עבורם $w - \sum a_i\zeta_i \in (p)$, לכן גם $\sigma_p(w) - \sum a_i\zeta^{pi} \in (p)$. מאחר שהאופיין של $D/(p)$ הוא p נקבל ש-$\sum a_i\zeta^{pi} - (\sum a_i\zeta^i)^p \in (p)$, ולכן

$$\sigma_p w - w^p = \sigma_p w - (\sum a_i\zeta^i)^p \in (p)$$

□

טענה 2.2.8. *לכל אידאל ראשוני P שמכיל את p מתקיים $\sigma_p P = P$.*

הוכחה. אם $w \in P$ אז $\sigma_p w - w^p \in (p) \subset P$ ו-$w^p \in P$, לכן $\sigma_p w \in P$, כלומר $\sigma_p P \subset P$. מאחר ש-$\sigma_p P$ ראשוני הוא גם מקסימלי ולכן יש שוויון.
$\square$

טענה 2.2.9. *יהי P אידאל ראשוני שמכיל את p. אז $1+P, \zeta+P, \dots, \zeta^{m-1}+P \in D/P$ שונים בזוגות.*

הוכחה. נחלק את $x^m - 1 = \prod(x-\zeta^i)$ ב-$x-1$ ונקבל ש-$1+\dots+x^{m-1} = \prod^{m-1}(x-\zeta^i)$. נציב $x=1$ ונקבל ש-$m = \prod^{m-1}(1-\zeta^i)$. לכן $m+P = \prod^{m-1}(1-\zeta^i+D)$. מאחר ש-$m$ ו-p זרים $m+P \neq P$ (אחרת $1 = am+bp \in P$), ולכן $\zeta_i + P \neq 1+P$ ל-$1 \le i \le m-1$. מכאן שאם $0 \le i < j \le m-1$ אז $\zeta^{i-j}+P \neq 1+P$, כלומר $\zeta^i + P \neq \zeta^j + P$. $\square$

משפט 2.2.10. *יהי f השלם החיובי המינימלי עבורו $p^f = 1 \mod m$ (ראינו שקיים כזה בהוכחת טענה 2.2.6). אז $(p) = \prod^g P_i$ כאשר הדרגה של P_i היא f ו-$g = \frac{\phi(m)}{f}$.*

הוכחה. לכל n, σ_p^n היא הזהות אםם היא מעבירה את ζ לעצמו, אםם $\zeta^{p^n} = z$ אםם $p^n = 1 \mod m$. לכן f הוא הסדר של σ_p.
נסמן ב-f_1 את המעלה של P_1. מאחר שהסדר של החבורה הכפלית של D/P_1 הוא $f_1 - 1$ נקבל ש-$w^{p^{f_1}} - w \in P_1$ לכל $w \in D$. החבורה הכפלית ציקלית, לכן יש איבר שסדרו $p^{f_1}-1$ ולכן f_1 הוא השלם החיובי המינימלי עבורו $w^{p^{f_1}} - w \in P_1$ לכל $w \in D$.
לפי טענה 2.2.7 $\sigma_p^k(w) - \sigma_p^{k-1} w^p \in P_1$ ובאינדוקציה אם $\sigma_p^{k-1}w - w^{p^{k-1}} \in P_1$ אז $\sigma_p^{k-1}w^p - (w^p)^{p^{k-1}} \in P_1$ לכן $\sigma_p^{k-1}w^p - w^{p^k} \in P_1$ ולכן $\sigma_p^k w - w^{p^k} \in P_1$. בפרט $w - w^{p^f} \in P_1$. מכאן ש-$f \ge f_1$.
מאחר ש-$\zeta^{p^{f_1}} + P_1 = \zeta + P_1$ נקבל מטענה 2.2.9 ש-$p^{f_1} = 1 \mod m$, ולכן $f \le f_1$. מכאן ש-$f = f_1$, כלומר הדרגה של P_1 היא f. לכל ה-P_i דרגה f ואינדקסי ההסתעפות שלהם 1. מ-$efg = \phi(m)$ נקבל ש-$g = \frac{\phi(m)}{f}$. $\square$

טענה 2.2.11. *נניח ש-m ראשוני. אז האידאל $L = (1-\zeta)$ הוא ראשוני בעל מעלה 1 ו-$L^{m-1} = (m)$.*

הוכחה. כמו בהוכחת טענה 2.2.9 נקבל $m = \prod^{m-1}(1-\zeta^i)$. נסמן $u_i = \frac{1-\zeta^i}{1-\zeta} = 1+\cdots+\zeta^{i-1}$. מאחר ש-$m$ לא מחלק את i הם זרים, כלומר יש שלמים a, b עבורם $am + bi = 1$ ולכן $bi = 1 \mod m$. מכאן ש

$$u_i^{-1} = \frac{1-\zeta}{1-\zeta^i} = \frac{1-(\zeta^i)^b}{1-\zeta^i} = 1+\zeta^i+\cdots+\zeta^{i(b-1)}$$

הוא שלם אלגברי, לכן u_i הפיך ב-D ומכאן שגם $\prod u_i$ הפיך ב-D. מאחר ש-$m = (1-\zeta)^{m-1}\prod u_i$ נקבל ש-$L^{m-1} = (m)$.

כעת נרשום את L כמכפלה של ראשוניים, $L = \prod^g Q_i^{a_i}$. נקבל ש-$\prod^g Q_i^{a_i(m-1)} = (m)$. נסמן ב-$e, f$ את אינדקס ההסתעפות והמעלה המשותפים של ה-Q_i. אז $e = a_i(m-1)$, ומאחר ש-$efg = \phi(m) = m-1$ נקבל ש-$a_i fg = 1$ כלומר $a_i = f = g = 1$. מכאן ש-$L = Q_1$, לכן הוא ראשוני, והדרגה שלו היא 1.

□

למה 2.2.12. *אם* n, m *זרים אז* $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$.

הוכחה. $\zeta_m = \zeta_{mn}^n \in \mathbb{Q}(\zeta_{mn})$ ובאותו אופן $\zeta_n \in \mathbb{Q}(\zeta_{mn})$. מאחר ש-$m, n$ זרים יש שלמים u, v כך ש-$um + vn = 1$, לכן $\zeta_{mn} = \zeta_{mn}^{um}\zeta_{mn}^{vn} = \zeta_n^u\zeta_m^v \in \mathbb{Q}(\zeta_n, \zeta_m)$.

□

בטענה הבאה ובהוכחתה אידאלים ראשיים יהיו ביחס ל-$\mathbb{Q}(\zeta_p, \zeta_m)$.

טענה 2.2.13. *יהי* D *חוג השלמים האלגבריים של* $\mathbb{Q}(\zeta_p, \zeta_m)$. *אז* $(p) = \prod^g P_i^{p-1}$ *כאשר* P_i *הם אידאלים ראשונים שונים זה מזה בעלי מעלה* f *ו-* $g = \frac{\phi(m)}{f}$. *המעלה* f *היא השלם החיובי המינימלי עבורו* $p^f = 1 \mod m$.

הוכחה. נסמן ב-D_m, D_p את חוגי השלמים האלגבריים ב-$\mathbb{Q}(\zeta_m), \mathbb{Q}(\zeta_p)$ בהתאמה. לפי טענה 2.2.11 $pD_p = ((1-\zeta_p)D_p)^{p-1} = (1-\zeta_p)^{p-1}D_p$. נרשום $(1-\zeta_p)D = \prod^t P_i^{a_i}$ עבור P_i ראשוניים שונים זה מזה ב-D. מאחר ש-$D_p \subset D$ ה-u_i מהוכחת טענה 2.2.11 הפיכים גם ב-D, ולכן כמו שם $pD = (1-\zeta_p)^{p-1}D = \prod^t P_i^{a_i(p-1)}$. נסמן $e' = a_i$ (זה זהה לכל i כי אינדקס ההסתעפות של כל הראשוניים במכפלה הזו זהה), אז $pD = (\prod^t P_i)^{e'(p-1)}$. נסמן ב-$f'$ את המעלה המשותפת לראשוניים האלה.

לפי משפט 2.2.10 $pD_m = \prod^g \tilde{P}_i$ כאשר $\tilde{P}_i$ ראשוניים ב-D_m בעלי מעלה $f = \frac{\phi(m)}{g}$. לכל i יהי Q_i אידאל ראשוני ב-D עבורו $\tilde{P}_i = Q_i \cap D_m$ (לפי טענה 1.2.27 קיים כזה). אז $(p) \subset Q_i$, ולכן $P_{j_i} = Q_i$. מכאן שההעתקה $P \mapsto P \cap D_m$ מ-$\{P_i\}_{i=1}^t$ ל-$\{\tilde{P}_i\}_{i=1}^g$ היא על. (התמונה של כל איבר בתחום היא בטוח כי היא אידאל ראשוני ב-D_m שמכיל את (p)). לכן $g \geq t$. בנוסף ההעתקה $D_m/\tilde{P}_i \to D/P_{j_i}, x+\tilde{P}_i \mapsto x+P_{j_i}$ מוגדרת היטב וחח"ע (אם $x-y \in \tilde{P}_i$ אז $x-y \in P_{j_i}$ ואם $x-y \in P_{j_i}$ ו-$x, y \in D_m$ אז $x-y \in \tilde{P}_i = P_{j_i} \cap D_m$) לכן $f \leq f'$.
מהפירוק של (p) ומכך ש-$\phi(pm) = [\mathbb{Q}(\zeta_m, \zeta_p) : \mathbb{Q}]$ נקבל ש-

$$(p-1)\phi(m) = \phi(pm) = e'(p-1)f't \geq e'(p-1)fg = e'(p-1)\phi(m)$$

כלומר $1 \leq e'$ ולכן $e' = 1$. מכאן שהאי שוויון הוא למעשה שוויון, כלומר $f'g = f't$. מאחר ש-$f' \geq f, t \geq g$ נקבל ש-$f' = f, t = g = \frac{\phi(m)}{f}$.

$\square$

3 יחס שטיקלברגר וחוק ההדדיות של אייזנשטיין

3.1 הנורמה של אידאל

נסמן ב-F שדה מספרים אלגבריים, ב-D את חוג השלמים שלו וב-A אידאל ב-D.

הגדרה 3.1.1. *הנורמה* $N(A)$ *של* A *היא מספר האיברים ב-*D/A.

למה 3.1.2. *אם* $A=\prod P_i^{a_i}$ *עבור* P_i *ראשוניים שונים זה מזה אז* $N(A)=\prod N(P_i)^{a_i}$.

הוכחה. עבור $i\neq j$ מתקיים $P_i^{a_i}+P_j^{a_j}=D$, לכן לפי טענה 1.1.10 $D/A\cong\bigtimes D/P_i^{a_i}$. לפי טענה 1.3.2 הנורמה של $P_i^{a_i}$ היא $N(P_i)^{a_i}$, ולכן

$$N(A)=\prod N(P_i^{a_i})=\prod N(P_i)^{a_i}$$

□

טענה 3.1.3. *אם* A,B *אידאלים אז* $N(AB)=N(A)N(B)$.

הוכחה. נרשום פירוק לראשוניים $A=\prod P_i^{a_i}, B=\prod Q_i^{b_i}$. אז $AB=\prod P_i^{a_i}\prod Q_i^{b_i}$. אם $P_i=Q_j$ אז נקבץ אותם ל-$P_i^{a_i+b_j}$. הנורמה של האידאל הזה היא $N(P_i)^{a_i+b_j}=N(P_i)^{a_i}N(Q_j)^{b_j}$, לכן גם אם יש $P_i=Q_j$ אפשר להפעיל את הלמה הקודמת ולקבל

$$N(AB)=\prod N(P_i)^{a_i}\prod N(Q_i)^{b_i}=N(A)N(B)$$

□

טענה 3.1.4. *נניח ש-*$F/\mathbb{Q}$ *נורמלית עם חבורת גלואה* G. *אז* $\prod_{\sigma\in G}\sigma(A)=(N(A))$.

הוכחה. נרשום $A=\prod P_i^{a_i}$, אז אגף שמאל הוא $\prod_i(\prod_{\sigma\in G}\sigma(P_i))^{a_i}$ ואגף ימין הוא $\prod_i(N(P_i))^{a_i}$ לכן מספיק להראות את הטענה ל-$A=P$ ראשוני.
יהיו $P_i=\sigma_i P$ g האידאלים הראשונים השונים ב-$\{\sigma(P):\sigma\in G\}$, אז $(\sigma_i)^g$ מערכת נציגים למנה של G ביחס שקילות לפיו שני איזומורפיזמים שקולים אםם התמונות של P לפיהם שוות. σ,τ שקולים אםם $\sigma\tau^{-1}P=P$, לכן מספר האיברים בכל מחלקת שקילות הוא $|G(P)|$, כאשר

$$G(P)=\{\sigma\in G:\sigma(P)=P\}$$

, ולכן $|G|=g|G(P)|$. מאחר שה-P_i הם האידאלים השונים המכילים את p (לפי טענה 1.3.4) כאשר $P_i\cap\mathbb{Z}=(p)$, נקבל ש $efg=n=|G|$ ולכן $|G(P)|=ef$. מכאן ש

$$\prod\sigma(P)=\prod^{g}P_i^{ef}=(p)^f=(p^f)=(N(P))$$

□

טענה 3.1.5. *נניח ש-$F/\mathbb{Q}$ נורמלית עם חבורת גלואה G. יהי D $\alpha \in$ ויהי $A = (\alpha)$. אז* $N(A) = |N(\alpha)|$.

הוכחה.

$$(N(A)) = \prod \sigma(A) = \prod \sigma((\alpha)) = \prod(\sigma\alpha) = (\prod \sigma\alpha) = (N(\alpha))$$

לכן $N(A)$ ו-$N(\alpha)$ חברים ב-D. מאחר ששניהם שלמים הם נבדלים זה מזה בסימן, ובגלל ש-$N(A)$ חיובי $N(A) = |N(\alpha)|$. $\square$

3.2 סימן שארית של חזקה

יהי m שלם חיובי. נסמן ב-D_m את חוג השלמים של $\mathbb{Q}(\zeta_m)$. יהי $P \not\ni m$ אידאל ראשוני ב-D_m ויהי $q = N(P) = |D_m/P|$. לפי טענה 2.2.9 המחלקות $1 + D_m, \zeta_m + D_m, \ldots, \zeta_m^{m-1} + D_m$ שונות זו מזו ו-$q = 1 \mod m$.

טענה 3.2.1. *יהי $a \in D_m - P$. קיים i יחיד מודולו m עבורו $a^{\frac{q-1}{m}} - \zeta_m^i \in P$.*

הוכחה. מאחר שהחבורה הכפלית של השדה הסופי D_m/P מסדר $q-1$ מתקיים

$$\prod_{i=0}^{m-1}(a^{\frac{q-1}{m}} - \zeta_m^i) = a^{q-1} - 1 \in P$$

ובגלל ש-P ראשוני קיים $0 \le i < m$ עבורו $a^{\frac{q-1}{m}} - \zeta_m^i \in P$. אם $i \ne j \mod m$ אז לפי טענה 2.2.9 $\zeta_m^i - \zeta_m^j \notin P$, ומכאן היחידות. $\square$

הגדרה 3.2.2. *יהי $a \in D_m$. נגדיר את סימן השארית של החזקה ה-m-ית, $(a/P)_m$, בתור 0 אם $a \in P$ ובתור ζ_m^i עם i מהטענה הקודמת, כלומר בתור שורש היחידה מסדר m היחיד עבורו $a^{\frac{N(P)-1}{m}} - (a/P)_m \in P$.*

עבור אידאל A נסמן ב-$a = b(A)$ שוויון מודולו A, כלומר $a = b(A)$ אםם $b - a \in A$.

טענה 3.2.3. *1. $(a/P)_m = 1$ אםם $x^m = a(A)$ פתירה ב-D_m.*
2. $a^{\frac{N(P)-1}{m}} = (a/P)_m(P)$.
3. $(ab/P)_m = (a/P)_m(b/P)_m$.
4. אם $a = b(P)$ אז $(a/P)_m = (b/P)_m$.

הוכחה. 1. נניח שיש $x \in D_m$ כך ש-$x^m = a(P)$. אז $a^{\frac{N(P)-1}{m}} = x^{N(P)-1} = 1(P)$ מאחר שהסדר של החבורה הכפלית של D_m/P הוא $N(P)-1$.
נניח שסמל השארית הוא 1, כלומר ש-$a^{\frac{N(P)-1}{m}} = 1(P)$. יהי $x+P$ יוצר של החבורה הכפלית הציקלית של D_m/P, ונרשום $a = x^k(P)$. אז $x^{\frac{k(N(P)-1)}{m}} = 1(P)$. מאחר שהסדר של x הוא $N(P)-1$ נקבל ש-$k = mn$ עבור n שלם, לכן $a = (x^n)^m(P)$.
2. חלק מההגדרה.
3. אם $ab \in P$ אז בגלל שהוא ראשוני אחד מ-a, b ב-P, לכן (אם זה a) $(a/P)_m = 0$ ובגלל ש-$(ab/P)_m = 0$ נקבל את השוויון. אחרת $a, b \notin P$ ו

$$(ab)^{\frac{N(P)-1}{m}} = a^{\frac{N(P)-1}{m}} b^{\frac{N(P)-1}{m}} = (a/P)_m(b/P)_m(P)$$

מכפלת סמלי השארית היא שורש היחידה, לכן מתקיים השוויון.
4. אם אחד מבין a, b שייך ל-P אז גם השני ושני סמלי השאריות הם 0.
אחרת, $(a/P)_m = a^{\frac{N(P)-1}{m}} = b^{\frac{N(P)-1}{m}}$ ולכן $(b/P)_m = (a/P)_m$.

$\square$

טענה 3.2.4 $(\zeta_m/P)_m = \zeta_m^{\frac{N(P)-1}{m}}$

הוכחה. שני האגפים הם שורשי יחידה מסדר m והם באותה מחלקה של D_m/P, לכן לפי טענה 2.2.9 (ההסתמכות שלה על הנתון הנוסף נותנת רק ש-$m \notin P$, מה שנתון גם פה) הם שווים. $\square$

יהיו A, B אידאלים ב-D (חוג השלמים של שדה מספרים אלגבריים כלשהו). אם $A+B \neq D$ אז קיים אידאל ראשוני P כך ש-$A+B \subset P$, לכן $A, B \subset P$ ולכן P מופיע בהצגות של שניהם כמכפלות ראשוניים. אם קיים ראשוני P שמופיע בהצגות של שניהם כמכפלות ראשוניים אז $A, B \subset P$ ולכן גם $A+B \subset P$, ובפרט $A+B \neq D$.
זה מוביל להגדרה הבאה.

הגדרה 3.2.5 *אידאלים A, B בחוג שלמים D של שדה מספרים אלגבריים נקראים זרים אם $A+B = D$, או באופן שקול אם לא קיים P ראשוני שמופיע בהצגות של שניהם כמכפלת ראשוניים.*

נרחיב את ההגדרה של סימן השארית כדי שנוכל לדבר על $(a/b)_m$ לכל b עבורו $(b), (m)$ זרים.

הגדרה 3.2.6 *יהי A אידאל שזר ל-(m). נרשום פירוק לראשוניים $A = \prod P_i$. ל-$a \in D_m$ נגדיר $(a/A)_m = \prod (a/P_i)_m$.*
אם $b \in D_m$ מקיים ש-$(m), (b)$ זרים נגדיר $(a/b)_m = (a/(b))_m$.

טענה 3.2.7 *יהיו A, B אידאלים שזרים ל-(m). אז*
1. $(ab/A)_m = (a/A)_m (b/A)_m$.
2. $(a/AB)_m = (a/A)_m (a/B)_m$.
3. *אם (a) זר ל-A ויש פתרון ב-D_m ל-$x^m = a(A)$ אז $(a/A)_m = 1$.*

הוכחה. נרשום פירוקים לראשוניים $A = \prod P_i, B = \prod Q_i$.
.1

$$(ab/A)_m = \prod (ab/P_i)_m = \prod (a/P_i)_m \prod (b/P_i)_m = (a/A)_m (b/A)_m$$

.2

$$(a/AB)_m = \prod (a/P_i)_m \prod (a/Q_i)_m = (a/A)_m (a/B)_m$$

3. קיים פתרון למשוואה הנתונה. לכל i, מאחר ש-$A \subset P_i$, הוא פותר גם את $x^m = a(P_i)$ ולכן $(a/P_i)_m = 1$. מכאן ש $(a/A)_m = \prod (a/P_i)_m = 1$. $\square$

מעתה נאמץ רישום מעריכי של אוטומורפיזמים, כלומר נרשום a^σ, A^σ במקום $\sigma a, \sigma A$.

טענה 3.2.8 *יהי A אידאל שזר ל-(m) ותהי $\sigma \in G$. אז $(a/A)_m^\sigma = (a^\sigma/A^\sigma)_m$.*

הוכחה. נרשום פירוק לראשוניים $A = \prod P_i$, אז $(a^\sigma/A^\sigma)_m = \prod(a/P_i)^\sigma_m, (a/A)^\sigma_m =$ $\prod(\alpha^\sigma/P_i^\sigma)$ ולכן מספיק להראות את הטענה ל-$A = P$ ראשוני. לפי ההגדרה $(a/P)_m(P) = a^{\frac{N(P)-1}{m}}$, לכן $(a/P)^\sigma_m(P^\sigma) = (a^\sigma)^{\frac{N(P)-1}{m}}$. מאחר ש-$N(P) = N(P^\sigma)$ אגף שמאל שקול ל-$(a^\sigma/P^\sigma)_m$ מודולו P^σ, כלומר $(a/P)^\sigma_m(P^\sigma) = (a^\sigma/P^\sigma)_m$ ומאחר ששניהם שורשי יחידה מסדר m הם שווים. $\square$

יהי $l \neq 2$ ראשוני. ניזכר שב-D_l מתקיים $(l) = (1-\zeta_l)^{l-1}$ ו-$(1-\zeta_l)$ הוא אידאל ראשוני ממעלה 1 (טענה 2.2.11).

הגדרה 3.2.9. $0 \neq a \in D_l$ *ששקול לשלם מודולו* $(1-\zeta_l)^2$ *ושמקיים* $(a), (l)$ *זרים נקרא פרימרי.*

כעת נוכל לנסח את חוק ההדדיות של אייזנשטיין. יתרת העבודה תוקדש להוכחתו ולמסקנות ממנו.

משפט 3.2.10. *יהיו* l *ראשוני אי זוגי,* a *שלם שזר לו ו-*$\alpha \in D_l$ *איבר פרימרי. נניח ש-*$(a), (\alpha)$ *זרים. אז* $(a/\alpha)_l = (\alpha/a)_l$.

3.3 יחס שטיקלברגר

נחקור את הפירוק לראשוניים של איברים מצורה מסוימת, שנקראים סכומי גאוס. לסכומים אלה יש שימושים רבים בתורת המספרים ובתורת ההצגות, וניעזר בהם לצורך הוכחת יחס שטיקלברגר.

הגדרה 3.3.1. *אפיין כפלי על שדה F הוא הומומורפיזם מהחבורה הכפלית של F לזו של $\mathbb{C}$. אפיין חיבורי הוא הומומורפיזם מהחבורה החיבורית של F לחבורה הכפלית של $\mathbb{C}$.*

יהי P אידאל ראשוני ב-D_m, חוג השלמים של $\mathbb{Q}(\zeta_m)$, ונניח ש-$m \notin P$. נרשום $P \cap \mathbb{Z} = (p)$ ו-$N(P) = q = p^f$. נסמן את השדה הסופי D_m/P ב-F. אז $p^f = 1 \mod m$.
לכל $0 \neq t = \gamma + P \in F$ נגדיר $\chi_P(t) = (\gamma/P)_m^{-1}$. לפי החלק הרביעי של טענה 3.2.2 זו פונקציה מוגדרת היטב, ולפי חלק 3 של אותה טענה היא אפיין כפלי. סמל שארית הוא שורש יחידה הוא בעל ערך מוחלט 1, ולכן $\chi_P(t)$ שווה גם ל-$\overline{(\gamma/P)_m}$.
נגדיר $\mathrm{tr} : F \to \mathbb{Z}_p$ ע"י $\mathrm{tr}(t) = \sum_{i=0}^{f-1} t^{p^i}$ (זו העקבה של $F/\mathbb{Z}_p$), ואפיין חיבורי ψ ע"י $\psi(t) = \zeta_p^{\mathrm{tr}(t)}$.
כעת נגדיר $g(P) = g(\chi_P, \psi) = \sum_{t \in F} \chi_P(t)\psi(t) \in \mathbb{Q}(\zeta_m, \zeta_p)$.
סכום כזה נקרא סכום גאוס על F ששייך ל-χ_P. נגדיר גם $\Phi(P) = g(P)^m$.

טענה 3.3.2. *מתקיים*
1. $|g(P)|^2 = q$.
2. $\Phi(P) \in \mathbb{Q}(\zeta_m)$.

הוכחה.
1. לשם פשטות נשמיט את הסימונים שמתייחסים לתלות ב-P. נסמן $g_a = \sum_{t \in F} \chi(t)\psi(at)$. אם $a \neq 0$ אז $t \mapsto at$ חח"ע ועל לכן נקבל

$$\chi(a)g_a = \chi(a)\sum_{t \in F}\chi(t)\psi(at) = \sum \chi(at)\psi(at) = g$$

ו $\overline{g_a} = \overline{g/\chi(a)} = \chi(a)\overline{g}$ כלומר $|g_a|^2 = \chi(a)\overline{g}g/\chi(a) = |g|^2$. אם $a = 0$ יהי b עבורו $(b/P) \neq 1$, אז $\chi(b) \neq 1$. מאחר ש-$t \mapsto bt$ חח"ע ועל נקבל

$$\chi(b)g_a = \chi(b)\sum \chi(t)\psi(0) = \chi(b)\sum \chi(t) = \sum \chi(bt) =$$

$$= \sum \chi(t) = \sum \chi(t)\psi(0) = g_a$$

ולכן $g_a = 0$. מכאן ש-$\sum_a |g_a|^2 = (q-1)|g|^2$.
מצד שני

$$|g_a|^2 = \sum_x \chi(x)\psi(ax)\sum_y \overline{\chi(y)}/\psi(by) =$$

$$= \sum_x \sum_y \chi(x)\overline{\chi(y)}\psi(ax - ay)$$

נסכום ונקבל

$$(q-1)|g|^2 = \sum_a |g_a|^2 = \sum_a \sum_x \sum_y \chi(x)\overline{\chi(y)}\psi(a(x-y)) =$$

$$= \sum_x \sum_y \chi(x)\overline{\chi(y)} \cdot \sum_a \psi(a(x-y))$$

עבור $x = y$ כל מחובר בסכום האחרון הוא 1 לכן הסכום הוא q. $a \mapsto a(x-y)$ חח"ע ועל עבור $x \neq y$ לכן במקרה הזה $\sum \psi(a(x-y)) = \sum \psi(a)$. יהי t שעבורו $\psi(t) \neq 1$. מאחר ש-$a \mapsto a+t$ חח"ע ועל $\psi(t)\sum \psi(a) = \sum \psi(a+t) = \sum \psi(a)$ ולכן $\sum \psi(a) = 0$. מכאן ש

$$(q-1)|g|^2 = \sum_x \chi(x)\overline{\chi(x)}q = (q-1)q$$

ומכאן התוצאה.

2. חבורת גלואה $G = G(\mathbb{Q}(\zeta_{mp}), \mathbb{Q})$ היא חבורת האוטומורפיזמים מהצורה σ_c עם $\gcd(c, pm) = 1$. מאחר ש-$\sigma_c|_{\mathbb{Q}}$ היא הזהות ו-$\sigma_c(\zeta_m) = \sigma_c(\zeta_{mp}^p) = \zeta_m^c$ נקבל ש-$\sigma_c|_{\mathbb{Q}(\zeta_m)}$ היא הזהות אםם $c = 1(m)$. באותו אופן $\sigma_c|_{\mathbb{Q}(\zeta_p)}$ היא הזהות אםם $c = 1(p)$.
מכאן שאם נראה ש-$\Phi(P)^{\sigma_c} = \Phi(P)$ לכל $c = 1(m)$ נקבל ש-$\Phi(P) \in \mathbb{Q}(\zeta_m)$.
יהי $c = 1(m)$. $\chi_P(t) \in \mathbb{Q}(\zeta_m)$ ו $\psi(t)^{\sigma_c} = \psi(t)^c = \psi(tc)$ לכן

$$g(P)^{\sigma_c} = \sum \chi_P(t)\psi(ct) = \chi_P(c)^{-1} \sum \chi_P(ct)\psi(ct) = \chi_P(c)^{-1} g(P)$$

ומכאן

$$\Phi(P)^{\sigma_c} = \chi_P(c)^{-m}\Phi(P) = \Phi(P)$$

כנדרש.

$\square$

יהי K שדה מספרים אלגבריים, ונניח ש-$K/\mathbb{Q}$ נורמלית עם חבורת גלואה G. לכל $(a(\sigma))_{\sigma \in G}$ שלמים נגדיר $\sum_{\sigma \in G} a(\sigma)\sigma : K \to K$ ע"י

$$\alpha^{\sum a(\sigma)\sigma} = \prod_{\sigma \in G} (\alpha^\sigma)^{a(\sigma)}$$

אם A אידאל נגדיר את התמונה שלו ע"י סכום כזה באותו אופן:

$$A^{\sum a(\sigma)\sigma} = \prod_{\sigma \in G} (A^\sigma)^{a(\sigma)}$$

כעת נוכל לנסח את יחס שטיקלברגר:

משפט 3.3.3. *יהי* $m \notin P \subset D_m$ *אידאל ראשוני. אז* $(\Phi(P)) = P^{\sum_{t \in U_m} t\sigma_t^{-1}} = \prod_{t \in U_m} (P^{\sigma_t^{-1}})^t$.

3.4 הוכחת יחס שטיקלברגר

נתחיל בתוצאות מתורת המספרים האלמנטרית שנזדקק להן בהמשך.

למה 3.4.1 (פיתוח לפי p). *יהי $1 < p \in \mathbb{Z}$. כל שלם חיובי ניתן לכתיבה באופן יחיד כ-$\sum_{i=0}^{n} a_i p^i$ עבור $0 \le a_i < p$.*

הוכחה. יהי a שלם חיובי. יש שלם אי שלילי יחיד n כך ש-$p^n \le a < p^{n+1}$. יש $a_n, 0 \le r < p^n$ כך ש-$a = a_n p^n + r$. מתקיים $a_n \le p$ כי $a_n p^n + r < p^{n+1}$. נעשה ל-r מה שעשינו ל-a, ונמשיך ככה כדי לקבל את ההצגה הרצויה של a. נסיים במספר סופי של צעדים כי בכל שלב שבו השארית אינה 0 הביטוי שהוא לא השארית גדל לפחות ב1.
נניח ש-$\sum b_i p^i = \sum a_i p^i$ עבור $0 \le a_i, b_i < p$. אז $a_0 - b_0 = \sum_{i \ge 1} b_i p^i - \sum_{i \ge 1} a_i p^i$, כלומר ההפרש מתחלק ב-$p$ ובגלל שערכו המוחלט קטן מ-p הוא שווה ל0. מכאן ש-$a_0 = b_0$. נחסר את האיבר הזה משני האגפים ונמשיך באותו אופן, וכך נקבל ש-$a_i = b_i$. □

הגדרה 3.4.2. *יהי $q = p^f$. אם $0 \le a < q-1$ נרשום $a = \sum_{i=0}^{f-1} a_i p^i, 0 \le a_i < p$ ונגדיר $S(a) = \sum a_i$. אם a שלם חיובי כלשהו נגדיר $S(a) = S(r)$ עבור שארית החלוקה r של a ב-$q-1$.*

למה 3.4.3. $S(a) = (p-1)\sum_{i=0}^{f-1} \langle \frac{p^i a}{q-1} \rangle$

הוכחה. כל אגף נשאר זהה אם מציבים בו $a + (q-1)k$ במקום a, לכן מספיק להראות את השוויון במקרה ש-$0 \le a < q-1$.
נרשום $a = \sum_{i=0}^{f-1} a_i p^i, 0 \le a_i < p$. מאחר ש-$p^f = q = 1 \mod (q-1)$ נקבל ש-$pa = a_{f-1} + \sum_{i=1}^{f-1} a_{i-1} p^i \mod q$ ובאופן כללי $p^k a = a_{f-k} + a_{f-k+1} p + \cdots + a_{f-k-1} p^{f-1} \mod (q-1)$. אגף ימין של השקילות הזו קטן מ-$q-1$, לכן שארית החלוקה של $p^k a$ ב-$q-1$ היא האגף הימני. מאחר שהשארית הזו היא גם $(q-1)\langle \frac{p^k a}{q-1} \rangle$ נקבל את תוצאת הלמה. □

למה 3.4.4. $\sum_{a=1}^{q-2} S(a) = \frac{f(q-1)(q-2)}{2}$

הוכחה. לכל $1 \le a \le q-2$ נרשום $a = \sum a_i p^i, 0 \le a_i < p$. מתקיים $q-1 = \sum_{i=0}^{f-1} (p-1) p^i$ ולכן $q-1-a = \sum (p-1-a_i) p^i$ ולכן $S(a) + S(q-1-a) = f(p-1)$. מכאן ש $\sum S(a) + \sum S(q-1-a) = f(p-1)(q-2)$ כלומר (שני הסכומים באגף שמאל שווים) $\sum S(a) = \frac{f(p-1)(q-2)}{2}$. □

נסמן ב-p ראשוני ב-$\mathbb{Z}$, m שלם שזר ל-p, f השלם החיובי המינימלי שמקיים $p^f = 1 \mod m$, $q = p^f$ ו-$\lambda = 1 - \zeta_p$. מתקיים $D_m \supset D_{q-1} \supset D_{(q-1)p}$ מאחר שאם $a = bc$ אז $\zeta_b = \zeta_a^c$. יהיו $P \subset D_m$ אידאל ראשוני שמכיל את p, $B \subset D_{q-1}$ אידאל ראשוני שהחיתוך שלו עם D_m הוא P (קיים כזה לפי טענה 1.2.27), ו $\mathscr{P} \subset D_{(q-1)p}$ אידאל ראשוני שמכיל את B. כשנרשום סדר של קבוצה שאינה אידאל בחוג מסוים נתכוון לסדר של האידאל שנוצר על ידה.

למה 3.4.5. *מתקיים*
1. $\mathrm{ord}_{\mathscr{P}}(pD_{(q-1)p}) = p-1$.
2. $\mathrm{ord}_{\mathscr{P}}(\lambda) = 1$.
3. $\mathrm{ord}_{\mathscr{P}}(P) = p-1$.

הוכחה. 1. $D_{(q-1)p}$ הוא חוג השלמים של $\mathbb{Q}(\zeta_p, \zeta_{q-1}) = \mathbb{Q}(\zeta_{(q-1)p})$, לכן הטענה נובעת מטענה 2.2.13.
2. לפי טענה 2.2.11 וטענה 2.2.13
$pD_{p(q-1)} = (pD_p)D_{p(q-1)} = \lambda^{p-1}D_{p(q-1)} = \prod^h \mathscr{P}_i^{p-1}$ ואחד מהגורמים הוא $\mathscr{P}$. ע"י פירוק לראשוניים נקבל ש-$\lambda D_{(q-1)p} = \prod \mathscr{P}_i$ ומכך נובעת הטענה.
3. לפי משפט 2.2.10 $pD_m = P\prod_{i=1}^{h-1} P_i$ עבור P_i ראשוניים ב-D_m, לכן
$P\prod^{h-1} P_iD_{(q-1)p} = pD_{(q-1)p} = \prod^h \mathscr{P}_i^{p-1}$ (גם במכפלה של משפט 2.2.10 יש h גורמים מאחר ששניהם שווים ל-$\frac{\phi(m)}{f}$). מאחר ש-P_i ו-P זרים בזוגות ב-D_m גם $P_iD_{(q-1)p}, PD_{(q-1)p}$ זרים בזוגות ב-$D_{(q-1)p}$ ולכן בפירוק של כל אחד מהם למכפלת ראשוניים יש רק אחד מה-$\mathscr{P}_i$. מאחר ש-$PD_{(q-1)p} \subset \mathscr{P}$ האידאל הזה שווה ל-$\mathscr{P}^{p-1}$, ומכאן הטענה. □

למה 3.4.6. $D_m/P \cong D_{q-1}/B$

הוכחה. ההומומורפיזם $x+P \mapsto x+B$ מוגדר היטב וחח"ע, כי אם $x-y \in P$ אז $x-y\in B$ ואם $x-y \in B, x,y \in D_m$ אז $x-y \in B\cap D_m = P$. לפי משפט 2.2.10 $|D_{q-1}/B| = p^{f'}$ כאשר f' הוא השלם החיובי המינימלי עבורו $p^{f'} = 1 \mod (q-1)$. מאחר ש-$q=p^f$ נקבל $|D_{q-1}/B| = p^{f'} = p^f = |D_m/P|$ ולכן ההומומורפיזם הזה הוא גם על, כלומר איזומורפיזם. □

$q-1 \notin B$ כי אחרת מהזרות של $p, q-1$ נובע ש-$1 = ap + b(q-1) \in B$ וזה לא ייתכן. לכן אפשר לדבר על $(a/B)_{q-1}$ ל-$a \in D_{q-1}$. בהמשך הסעיף נסמן אותו פשוט ב-(a/B).

למה 3.4.7. לכל $a \in D_m$ *מתקיים* $(a/B)^{\frac{q-1}{m}} = (a/P)_m$.

הוכחה. אם $a \in P$ אז $a \in B$ ושני האגפים מתאפסים. אחרת, $(a/B)^{\frac{q-1}{m}}(B)$ כי $a^{\frac{q-1}{m}} = a$ $(a/B)(B)$. מאחר ש-$B = P\cap D_m$ ושני האגפים שייכים ל-D_m נקבל גם שהשקילות מתקיימת מודלו P, ומאחר שאגף ימין הוא שורש יחידה מסדר m נקבל את הנדרש. □

כעת נגדיר אפיין כפלי ω על $F = D_m/P \cong D_{q-1}/B$ ע"י $\omega(\gamma+B) = (\gamma/B)$ (הוא מוגדר היטב וכפלי לפי טענה 3.2.3).
לפי טענות 3.2.3 ו3.2.4 $(\zeta_{q-1}^i/B) = \zeta_{q-1}^i$.

הגדרה 3.4.8. *יהי a שלם אי שלילי. נגדיר* $g_a = g(\omega^{-a}, \psi) = \sum_{t\in F}\omega^{-a}(t)\psi(t)$, *כאשר* $\omega^{-a}(t) = \omega(t)^{-a}$.

מלמה 3.4.7 נובע שסכום גאוס $g(P)$ מהסעיף הקודם הוא $g_{\frac{q-1}{m}}$.
נסמן $s(a) = \mathrm{ord}_{\mathscr{P}}(g_a)$.

למה 3.4.9. $s(1) = 1$

הוכחה. נרשום $g_1 = \sum_{t\in F}\omega(t)^{-1}\zeta_p^{\mathrm{tr}(t)}$. יהי m_i שלם חיובי שמייצג את $\mathrm{tr}(\zeta_{q-1}^i + b) \in \mathbb{Z}_p$.
מאחר ש-$\zeta_p = 1-\lambda$ וכל מחלקה מיוצגת באופן יחיד על ידי חזקה של ζ_{q-1} נקבל

$$g_1 = \sum_{i=0}^{q-2}\zeta_{q-1}^{-i}(1-\lambda)^{m_i}$$

לפי נוסחת הבינום

$$(1-\lambda)^{m_i} = \sum_{j=0}^{m_i}\binom{m_i}{j}(-1)^j\lambda^j$$

ומאחר ש-$\lambda^j \in \mathscr{P}^2$ ל-$j \geq 2$ נקבל ש-$(1-\lambda)^{m_i} \equiv 1-m_i\lambda(\mathscr{P}^2)$. מכאן ומכך ש-$\sum_{i=0}^{q-2}\zeta_{q-1}^{-i} =$
$\sum_{j=1}^{q-1}\zeta_{q-1}^{j} = 0 \in \mathscr{P}^2$ נובע ש

$$g_1 \equiv -\sum_{i=0}^{q-2}\zeta_{q-1}^{-i}m_i\lambda(\mathscr{P}^2)$$

כעת $m_i \equiv \sum_{j=0}^{f-1}\zeta_{q-1}^{ip^j}(P^2)$ ולכן

$$g_1 \equiv -\sum_{i=0}^{q-2}\sum_{j=0}^{f-1}{\zeta_{q-1}}^{i(p^j-1)}\lambda = -\sum_{j=0}^{f-1}\sum_{i=0}^{q-2}{\zeta_{q-1}}^{i(p^j-1)}\lambda(\mathscr{P}^2)$$

מאחר שעבור $j > 0$ האיבר $\zeta_{q-1}^{p^j-1}$ הוא שורש יחידה שאינו 1 הסכום הפנימי מתאפס. עבור $j = 0$ מתקבל בסכום הפנימי $q-1$, ומאחר ש-$q = p^f \equiv 0(\mathscr{P}^2)$ נקבל ש-$g_1 \equiv -\lambda(\mathscr{P}^2)$ ולכן השקילות הזו מתקיימת גם מודלו $\mathscr{P}$. לפי למה 3.4.5 $-\lambda \in \mathscr{P} - \mathscr{P}^2$ ולכן גם $g_1 \in \mathscr{P} - \mathscr{P}^2$, כלומר $\mathrm{ord}_{\mathscr{P}}(g_1) = 1$.

□

לאפיינים כפליים χ_1, χ_2 נסמן $J(\chi_1,\chi_2) = \sum_{t\in F}\chi_1(t)\chi_2(1-t)$. איבר כזה נקרא סכום יעקובי (Jacobi) .

למה 3.4.10. ל-$1 \leq a,b < q-1$ *שעבורם* $1 \leq a+b < q-1$ *מתקיים* $g_a g_b = J(\omega^{-a},\omega^{-b})g_{a+b}$.

הוכחה.

$$g_a g_b = (\sum_x \omega^{-a}(x)\zeta_p^{\mathrm{tr}x})(\sum_y \omega^{-b}(x)\zeta_p^{\mathrm{tr}y}) = \sum_x\sum_y \omega^{-a}(x)o^{-b}(y)\zeta_p^{\mathrm{tr}(x+y)} =$$

$$= \sum_t(\sum_{x+y=t}\omega^{-a}(x)\omega^{-b}(y))\zeta_p^{\mathrm{tr}t}$$

עבור $t=0$ הסכום הפנימי מתאפס, כי הוא שווה ל-$\omega^{-b}(-1)\sum_x \omega^{-a}(x)\omega^{-b}(x)$ וכל שורש יחידה מסדר $q-1$ הוא התמונה של איבר אחד בדיוק על ידי האפיין הכפלי $x\mapsto \omega^{-a}(x)\omega^{-b}(x)$.
ל-$t\neq 0$ נגדיר $x'=\frac{x}{t}, y'=\frac{y}{t}$. אז $x'+y'=1$ לכל $x+y=t$, לכן הסכום הפנימי שווה ל

$$\sum_{x'+y'=1}\omega^{-a}(tx')\omega^{-b}(ty')=\omega^{-a}(t)\omega^{-b}(t)\sum_{x'}\omega^{-a}(x')\omega^{-b}(1-x')$$

ומכאן ש-

$$g_a g_b=\sum_t \omega^{-(a+b)}J(\omega^{-a},\omega^{-b})\zeta_p^{\mathrm{tr}t}=J(\omega^{-a},\omega^{-b})g_{a+b}$$

□

כעת נוכל להוכיח מספר תכונות של s.

למה 3.4.11. *לכל* $1\le a,b<q-1$ *שעבורם* $1\le a+b<q-1$ *מתקיים*
1. $s(a+b)\le s(a)+s(b)$.
2. $s(a+b)=s(a)+s(b) \mod (p-1)$.
3. $s(pa)=s(a)$.
4. $\sum_{a=1}^{q-2}s(a)=\frac{f(q-1)(p-2)}{2}$.

הוכחה. 1. לפי הלמה הקודמת

$$s(a+b)\le s(a+b)+\mathrm{ord}_{\mathscr{P}}(J(\omega^{-a},\omega^{-b}))=s(a)+s(b)$$

2. סכום יעקובי $J(\omega^{-a},\omega^{-b})$ שייך ל-$\mathbb{Q}(\zeta_{q-1})$. נרשום פירוק לראשוניים

$$J(\omega^{-a},\omega^{-b})D_{q-1}=B^m\prod P_i$$

אם $\mathrm{ord}_{\mathscr{P}}(J(\omega^{-a},\omega^{-b}))=0$ אז הטענה נובעת מהשוויון בלמה הקודמת. אחרת $\mathscr{P}\subset (J(\omega^{-a},\omega^{-b}))D_{(q-1)p}$ ועל ידי חיתוך עם D_{q-1} נקבל ש-$B\subset J(\omega^{-a},\omega^{-b})D_{q-1}$,
כלומר קיים $m>0$ כך שהפירוק לראשוניים הוא $J(\omega^{-a},\omega^{-b})D_{q-1}=B^m\prod P_i$.
כמו בהוכחת הסעיף השלישי של למה 3.4.5 $BD_{(q-1)p}=\mathscr{P}^{p-1}$, ולכן $J(\omega^{-a},\omega^{-b})D_{(q-1)p}=$ $\prod P_i\mathscr{P}^{m(p-1)}$ מאחר ש-$BD_{(q-1)p}, P_iD_{(q-1)p}$ זרים בזוגות
$\mathrm{ord}_{\mathscr{P}}(J(\omega^{-a},\omega^{-b}))=m(p-1)$ ומהלמה הקודמת נקבל את הנדרש.
3. מכך ש-$t^{p^f}\equiv 1\ (m)$ נובע ש $\mathrm{tr}\,t=\sum_{i=0}^{f-1}t^{p^i}=\sum_{i=1}^{f}t^{p^i}=\sum_{i=0}^{f-1}t^{p^{i+1}}=\mathrm{tr}(t^p)$ ולכן

$$g_{pa}=\sum\omega(t)^{-pa}\psi(t)=\sum\omega(t^p)^{-a}\psi(t^p)$$

מאחר ש-$t\mapsto t^p$ אוטומורפיזם נקבל ש-$g_{pa}=g_a$ ולכן $s(pa)=s(a)$.
4. לכל $1\le a<p$ מ-1 $s(a)\le as(1)=a$ ומ-2 $s(a)=a \mod (p-1)$, לכן $s(a)=a$.
לכל a מתקיים $\omega^a(-1)^2=1$ ובפרט $\omega^a(-1)$ ממשי. מכאן ש-

$$\overline{g_a}=\sum\overline{\omega^{-a}(t)\psi(t)}=\omega^{-a}(-1)\sum\overline{\omega^{-a}(-t)}\psi(-t)=\omega^{-a}(-1)g_{-a}$$

ומאחר ש- $\frac{1}{\omega^{-a}(-1)} = \omega^{-a}(-1)$ נקבל ש- $g_{-a} = \omega^{-a}(-1)\overline{g_a}$. מכאן, מכך ש- $g_{-a} = g_{q-1-a}$ ומטענה 3.3.2 נקבל ש-

$$g_a g_{q-1-a} = \omega^a(-1)\overline{g_{-a}}g_{q-1-a} = \omega^a(-1)p^f$$

משום ש- $\mathrm{ord}_{\mathscr{P}}(p) = p-1$ נובע ש- $s(a) + s(q-1-a) = f(p-1)$. נסכום מ- $a = 1$ עד $q-2$ ונקבל ש-

$$\sum_{a=1}^{q-2} s(a) = \frac{f(p-1)(q-2)}{2}$$

□

משפט 3.4.12. *לכל* $1 \le a < q$ *מתקיים* $s(a) = S(a)$.

הוכחה. ל- $1 \le a \le q-1$ נרשום $a = \sum_{i=0}^{f-1} a_i p^i$ עם $0 \le a_i < p$. מסעיפים 1 ו-3 בלמה הקודמת

$$s(a) \le \sum s(a_i p^i) = \sum s(a_i) = \sum a_i = S(a)$$

לפי למה 3.4.4 וסעיף 4 של הלמה הקודמת $\sum_{a=1}^{q-2} s(a) = \sum_{a=1}^{q-2} S(a)$ ולכן לכל $1 \le a < q-1$ מתקיים $s(a) = S(a)$. ל- $q-1$ שני האגפים הם 0 לכן השוויון מתקיים. □

טענה 3.4.13 $\mathrm{ord}_P(\Phi(P)) = \frac{m}{p-1} S(\frac{q-1}{m})$.

הוכחה. נרשום פירוק לראשוניים $\Phi(P)D_m = P^{\mathrm{ord}_P(\Phi(P))} \prod Q_i$, אז

$$\Phi(P)D_{(q-1)p} = (PD_{(q-1)p})^{\mathrm{ord}_P(\Phi(P))} \prod Q_i$$

ולכן לפי למה 3.4.5

$$\mathrm{ord}_{\mathscr{P}}(\Phi(P)) = \mathrm{ord}_P(\Phi(P))\mathrm{ord}_{\mathscr{P}}(PD_{(q-1)p}) = (p-1)\mathrm{ord}_P(\Phi(P))$$

לפי המשפט הקודם $\mathrm{ord}_{\mathscr{P}} g(P) = s(\frac{q-1}{m}) = S(\frac{q-1}{m})$ ומאחר ש- $\Phi(P) = g(P)^m$ נקבל ש $\mathrm{ord}_{\mathscr{P}}(\Phi(P)) = mS(\frac{q-1}{m})$, ומכאן התוצאה. □

לפי טענה 3.3.2 $|\Phi(P)|^2 = q^m = p^{fm}$. לכל אידאל ראשוני Q שמכיל את $\Phi(P)$ מתקיים $D_m/Q \subset D_m/(\Phi(P))$ ולכן הסדר של D_m/Q הוא חזקה של p, כלומר $p \in Q$.
אם P' הוא אידאל ראשוני ב- D_m שמכיל את p אז לפי טענה 1.3.4 יש אוטומורפיזם $\sigma_t \in G(\mathbb{Q}(\zeta_m), \mathbb{Q})$ כך ש- $P' = P^{\sigma_t^{-1}}$. לכל $1 \le t < m$ שזר ל- m נגדיר $P_t = P^{\sigma_t^{-1}}$.

למה 3.4.14 $\mathrm{ord}_{P_t}(\Phi(P)) = \frac{m}{p-1} S(t\frac{q-1}{m})$.

הוכחה. נרשום פירוק לראשוניים $\Phi(P) = P_t^o \prod Q_j$ עבור $Q_j \neq P_t$. אז $\Phi(P)^{\sigma_t} = P^o \prod Q_j^{\sigma_t}$ ולכן $\mathrm{ord}_{P_t}(\Phi(P)) = \mathrm{ord}_P(\Phi(P))^{\sigma_t}$. לפי משפט השארית יש t' כך ש-$t' = 1(p), t' = t(m)$. אז t' זר ל-m ולא מתחלק ב-p לכן הוא זר גם ל-mp, ולכן קיים $\sigma_{t'}$ כאוטומורפיזם של $\mathbb{Q}(\zeta_{mp})$. מתקיים

$$\sigma_{t'}(\zeta_m) = \sigma_{t'}(\zeta_{mp}^p) = \zeta_{mp}^{t'p} = \zeta_m^{t'} = \zeta_m^t$$

כי $t = t'(m)$ לכן $\sigma_{t'}(x) = \sigma_t(x)$ ל-$x \in \mathbb{Q}_{\zeta_m}$. באופן דומה

$$\sigma_{t'}(\zeta_p) = \zeta_p^{t'} = \zeta_p$$

כי $t' = 1(p)$, כלומר $\sigma_{t'}(x) = x$ ל-$x \in \mathbb{Q}(\zeta_p)$. מכאן

$$g(P)^{\sigma_{t'}} = (\sum \chi_P(x)\psi(x))^{\sigma_{t'}} = \sum \chi_P(x)^t \psi(x)$$

כלומר

$$\Phi(P)^{\sigma_t} = (\sum \chi_P(x)^t \psi(x))^m = g_a^m$$

כאשר $a = t(q-1)/m$. מכאן לפי משפט 3.4.12

$$\mathrm{ord}_P(\Phi(P)^{\sigma_t}) = \frac{\mathrm{ord}_{\mathscr{P}}(\Phi(P)^{\sigma_t})}{p-1} = \frac{m\mathrm{ord}_{\mathscr{P}}(g_a)}{p-1} = \frac{m}{p-1} S(a)$$

כנדרש.

□

טענה 3.4.15. *בסימוני משפט 2.2.10, יהי P אידאל מתוך האוסף (P_i) ונגדיר $G(P) = \{\sigma \in G : \sigma P = P\}$. אז $G(P)$ חבורה ציקלית שנוצרת ע"י σ_p.*

הוכחה. לפי טענה 2.2.8 $\sigma_p \in G(P)$. מהוכחת טענה 3.1.4 $g|G(P)| = \phi(m)$, ולכן $|G(P)| = f = |\langle\sigma_p\rangle|$ כלומר $G(P)$ נוצרת ע"י σ_p. □

יהיו $(t_i)^g$ שלמים שמייצגים את המחלקות של $U_m/(p + m\mathbb{Z})$, כלומר לכל $1 \leq t < m$ שזר ל-m מתקיים $t = t_i p^j \mod m$ עבור זוג יחיד (i, j) כך ש-$1 \leq i \leq g$, $0 \leq j < f$. לפי למה 3.4.14 הפירוק לראשוניים של $\Phi(P)$ הוא $P^{\frac{m}{p-1}\sum_{i=1}^g S(t_i \frac{q-1}{m})\sigma_{t_i}^{-1}}$ נסמן את המעריך ב-γ', אז לפי למה 3.4.3

$$\gamma' = m \sum_{i=1}^{g} (\sum_{j=0}^{f-1} \langle \frac{p^j t_i}{m} \rangle) \sigma_{t_i}^{-1}$$

לפי טענה 3.4.15 $\sigma_{p^j}(P) = P$ ולכן מתקיים $P^{\gamma'} = P^{\gamma}$ כאשר

$$\gamma = m \sum_i \sum_j \langle \frac{p^j t_i}{m} \rangle \sigma_{t_i}^{-1} \sigma_{p^j}^{-1} = m \sum_{t \in U_m} \langle \frac{t}{m} \rangle \sigma_t^{-1} = \sum_{t \in U_m} t \sigma_t^{-1}$$

בכך הוכחנו את יחס שטיקלברגר.

3.5 הוכחת חוק ההדדיות של אייזנשטיין

למה 3.5.1. *שורשי היחידה ב-$\mathbb{Q}(\zeta_m)$ עבור m ראשוני אי זוגי הם $\pm\zeta_m^i, i \in \{1,\dots,m\}$.*

הוכחה. חבורת שורשי היחידה סופית, מאחר שאם היא הייתה אינסופית אז סדרי שורשי היחידה היו לא חסומים, וזה לא ייתכן כי המעלה של $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ היא $\phi(n)$. יהי ζ_n יוצר של חבורת שורשי היחידה. מאחר שחזקה kית שלו היא ζ_m נקבל ש-$\frac{2\pi ik}{n} = \frac{2\pi i}{m} + 2\pi ik'$, לכן $(k-k'n)m = n$ ולכן m מחלק את n. שורשי היחידה מסדר 2 הם ± 1 ששייכים להרחבה, לכן באותו אופן (עם החלפה של m ב-2) נקבל ש-2 מחלק את n. מאחר ש-m ראשוני גם $2m$ מחלק את n.
בנוסף $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ ולכן $\phi(n) = \phi(m)$. נרשום $n = 2^a m^b k$ כאשר החזקות מקסימליות ונקבל ש-$\phi(m) = \phi(2^a)\phi(m^b)\phi(k)$. אם $b > 1$ או $a > 1$ או $k > 2$ אז אגף ימין גדול משמאל, ואם $k = 2$ אז החזקה a לא מקסימלית. מכאן ש-$n = 2m$, ומכאן התוצאה. □

למה 3.5.2. *יהי K שדה מספרים אלגבריים ויהיו $\sigma_1, \dots, \sigma_n$ ה-$n = [K : \mathbb{Q}]$ מונומורפיזמים של K לתוך $\mathbb{C}$. אם a שלם אלגברי המקיים ש-$|a^{\sigma_i}| \leq 1$ אז a שורש יחידה.*

הוכחה. a שורש של הפולינום במקדמים שלמים $f(x) = \prod(x - a^{\sigma_i})$. המקדם של x^m בפולינום מורכב מסכום של $\binom{m}{n}$ מה-a^{σ_i}, לכן חסום ע"י $\binom{m}{n}$. מאחר שהפולינום הוא במקדמים שלמים יש רק מספר סופי של aים כאלה. אבל כל חזקה של a מקיימת את הנתון, לכן $a^i = a^j$ עבור $i < j$, כלומר $a^{j-i} = 1$. □

כעת נגדיר את $\Phi(A)$ עבור A כלשהו שזר ל-(m) ב-D_m.

הגדרה 3.5.3. *יהי A אידאל ב-D_m שזר ל-(m). נגדיר $\Phi(A) = \prod \Phi(P_i)$, כש-$A = \prod P_i$ פירוק לראשוניים.*

טענה 3.5.4. *יהיו $A, B \subset D_m$ אידאלים שזרים ל-(m), $a \in D_m$ איבר שזר ל-(m), ו-$\gamma = \sum_{t\in U_m} t\sigma_t^{-1}$. אז*
1. *$\Phi(A)\Phi(B) = \Phi(AB)$.*
2. *$|\Phi(A)|^2 = (N(A))^m$.*
3. *$(\Phi(A)) = A^\gamma$.*
4. *$\Phi((a)) = \varepsilon(a)a^\gamma$ עבור $\varepsilon(a)$ שהפיך ב-D_m.*

הוכחה. 1. אם $A = \prod P_i, B = \prod Q_i$ אז $\Phi(AB) = \prod P_i \prod Q_i = \Phi(A)\Phi(B)$.
2.
$$|\Phi(A)|^2 = \prod |\Phi(P_i)|^2 = \prod |g(P_i)|^{2m} = \prod N(P_i)^m = N(A)^m$$
.
3. $(\Phi(A)) = \prod(\Phi(P_i)) = \prod P_i^\gamma = A^\gamma$.
4. מ-3 $(\Phi((a))) = (a)^\gamma = (a^\gamma)$, לכן $\Phi((a))$ ו-a^γ חברים.

□

מעתה נרשום פשוט $\Phi(a)$ במקום $\Phi((a))$. נצטרך לחקור עוד את $\varepsilon(a)$.

למה 3.5.5 *יהי A אידאל שזר ל-(m) ויהי σ אוטומורפיזם של $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. אז $\Phi(A)^\sigma = \Phi(A^\sigma)$.*

הוכחה. יהי P ראשוני. נרשום $g(P) = \sum (a/P)_m^{-1} \zeta_p^{\mathrm{tr}(a+P}$. יהי σ' אוטומורפיזם של $\mathbb{Q}(\zeta_m, \zeta_p)/\mathbb{Q}$ שהצמצום שלו ל-$\mathbb{Q}(\zeta_m)$ הוא σ ול-$\mathbb{Q}(\zeta_p)$ הוא הזהות (קיום אמור לנבוע מהוכחת 3.4.14). לפי טענה 3.2.8 $g(P)^{\sigma'} = \sum (a^\sigma/P^\sigma)_m^{-1} \zeta_p^{\mathrm{tr}(a+P)}$ מאחר ש-$\mathrm{tr}(a+P) \in \mathbb{Z}_p$ מתקיים $\mathrm{tr}(a^\sigma + P) = \mathrm{tr}(a+P)$. מכאן ש

$$g(P^\sigma) = \sum_a (a/P^\sigma)_m^{-1} \zeta_p^{\mathrm{tr}(a+P)} = \sum_{a^\sigma} (a^\sigma/P^\sigma)_m^{-1} \zeta_p^{\mathrm{tr}(a^\sigma+P)} = g(P)^{\sigma'}$$

ולכן $\Phi(P)^\sigma = \Phi(P^\sigma)$. באמצעות כפליות נקבל את התוצאה ל-A כלשהו. $\square$

למה 3.5.6 *לכל $a \in D_m$ מתקיים $|a^\gamma|^2 = |Na|^m$.*

הוכחה. האוטומורפיזם σ_{m-1} של $\mathbb{Q}(\zeta_m)$ מקיים $\sigma_{m-1}(\zeta_m) = \zeta_m^{-1} = \overline{\zeta_m}$ כלומר הוא הצמדה, לכן

$$|a^\gamma|^2 = a^\gamma a^{\gamma\sigma_{m-1}} = a^{\gamma(1+\sigma_{m-1})}$$

כש-1 היא הזהות. מתקיים

$$\gamma\sigma_{m-1} = (\sum t\sigma_t^{-1})\sigma_{m-1} = \sum t\sigma_{m-t}^{-1}$$

ומכאן ש $\gamma(1+\sigma_{m-1}) = \sum t\sigma_{m-t}^{-1} + \sum (m-t)\sigma_{m-t}^{-1} = m\sum \sigma_t^{-1}$. כעת $Na = \prod a^{\sigma_t^{-1}} = a^{\sum \sigma_t^{-1}}$ ומכאן התוצאה. $\square$

טענה 3.5.7 *יהי $a \in D_m$ שזר ל-(m). אז $\varepsilon(a) = \pm\zeta_m^i$ עבור i כלשהו.*

הוכחה. מתקיים $|\Phi(a)|^2 = (N((a)))^m$ לפי טענה 3.5.4 ולפי הלמה הקודמת $|a^\gamma|^2 = |Na|^m$. לפי טענה 3.1.5 מתקיים $N((a)) = |Na|$ ולכן $|\varepsilon(a)a^\gamma|^2 = |a^\gamma|^2$ כלומר $|\varepsilon(a)| = 1$. לפי למה 3.5.5 נקבל באותו אופן ש-$|\varepsilon(a)^\sigma| = 1$ לכל σ. מלמה 3.5.2 נקבל ש-$\varepsilon(a)$ שורש יחידה. מכאן לפי למה 3.5.1 ש-$\varepsilon(a) = \pm\zeta_m^i$. $\square$

כעת נוכל להתחיל את ההוכחה של חוק ההדדיות (משפט 3.2.10).

טענה 3.5.8 *יהיו $P, P' \subset D_m$ ראשוניים שזרים ל-(m). נניח גם ש-NP ו-NP' זרים. אז*

$$(\Phi(P)/P')_m = (NP'/P)_m$$

הוכחה. נסמן $q' = p'^{f'} = NP'$. מכיוון ש-$q' = 1(m)$ נקבל

$$g(P)^{q'} = \sum \chi_P(t)^{q'} \psi(t)^{q'} = \sum \chi_P(t) \psi(q't) =$$

$$= \sum \chi_P(t)/\chi_P(q')\psi(t) = (q'/P)_m g(P)(p')$$

ומאחר ש-$p' \in P'$ מתקיים השוויון גם מודולו P'. מצד שני

$$g(P)^{q'-1} = \Phi(P)^{\frac{q'-1}{m}} = (\Phi(P)/P')_m (P')$$

ומכאן ש

$$(\Phi(P)/P')_m = (NP'/P)_m (P')$$

מאחר ששני האגפים הם שורשי יחידה מסדר m ו-$m \notin P'$ הם שווים. $\square$

באמצעות כפליות נקבל את הטענה גם ל-P, P' לא ראשוניים.

טענה 3.5.9. *יהיו $A, B \subset D_m$ שזרים ל-(m) כך ש-NA, NB זרים, ונניח ש-$A = (a)$. אז*

$$(\varepsilon(a)/B)_m (a/NB)_m = (NB/a)_m$$

הוכחה. ראשית

$$(\Phi(a)/B)_m = (\varepsilon(a)/B)_m (a^\gamma/B)_m$$

לפי טענה 3.2.8 $(a^{t\sigma_t^{-1}}/B)_m = (a^{\sigma_t^{-1}}/B)_m^t = (a^{\sigma_t^{-1}}/B)_m^{\sigma_t} = (a/B^{\sigma_t})_m$. מכאן לפי טענה 3.1.4

$$(a^\gamma/B)_m = \prod_t (a^{t\sigma_t^{-1}}/B)_m = (a/\prod B^{\sigma_t})_m = (a/NB)_m$$

מהטענה הקודמת נקבל את התוצאה. $\square$

מעתה נניח ש-$m = l$ הוא ראשוני אי זוגי.

למה 3.5.10. *אם $A \subset D_l$ אידאל שזר ל-(l) אז $\Phi(A) = \pm 1(l)$.*

הוכחה. מספיק להראות ש-$\Phi(P) = -1(l)$ עבור $P \subset D_l$ ראשוני שזר ל-(l), כי אז נקבל את התוצאה מכפליות.
אכן

$$\Phi(P) = g(P)^l = \sum \chi_P(t)^l \psi(t)^l = \sum_{t \neq 0} \psi(lt) = \sum_{t \neq 0} \psi(t) = -1(l)$$

כשהשקילות האחרונה נובעת מכך ש-$\psi(0) = 1$ ו-$\sum \psi(t) = 0$ (ראינו את זה בהוכחת טענה 3.3.2). $\square$

טענה 3.5.11. *אם $a \in D_l$ פרימרי אז $\varepsilon(a) = \pm 1$.*

הוכחה. מאחר ש-$(1-\zeta_l)$ הוא הראשוני היחיד שמכיל את l מתקיים $(1-\zeta_l)^\sigma = (1-\zeta_l)$ לכל $\sigma \in G$. מכאן ש

$$((1-\zeta_l)^2)^\gamma \subset ((1-\zeta_l)^\gamma)^2 = (1-\zeta_l)^2$$

מאחר ש-$\Phi(a) = \varepsilon(a)a^\gamma$ נקבל מהלמה הקודמת ש-$\varepsilon(a)a^\gamma = \pm 1(l)$. מכיוון ש-$a = x(1-\zeta_l)^2$ עבור x שלם מתקיים

$$a^\gamma = x^\gamma = x^{\sum_{i=1}^{l-1} i} = x^{(l-1)l/2}(1-\zeta_l)^2$$

כעת l לא מחלק את x, כי אחרת $x \in (1-\zeta_l)^2$ ולכן גם $a \in (1-\zeta_l)^2$, וזה לא ייתכן כי $(1-\zeta_l)$ מופיע בפירוק לראשוניים של (l) ולכן לא יכול להופיע בזה של (a). מכאן ש-$x \in \mathbb{Z}/(l)$ שונה מ-0 ולכן $x^{l-1} = 1(l)$, ומאחר ש-$\mathbb{Z}/(l)$ שדה $x^{\frac{l-1}{2}} = \pm 1(l)$. לכן

$$a^\gamma = (\pm 1)^l = \pm 1(1-\zeta_l)^2$$

ומכאן ש-$\varepsilon(a) = \pm 1(1-\zeta_l)^2$. מטענה 3.5.7 $\varepsilon(a) = \pm\zeta_l^i$ עבור i כלשהו, לכן $\zeta_l^i = \pm 1(1-\zeta_l)^2$, כלומר

$$(1-(1-\zeta_l))^i = \pm 1(1-\zeta_l)^2$$

לכן

$$1 - i(1-\zeta_l) = \pm 1(1-\zeta_l)^2$$

אם הסימן הוא מינוס נקבל $i(1-\zeta_l) = 2(1-\zeta_l)^2$ לכן יש α עבורו $i(1-\zeta_l)+\alpha(1-\zeta_l)^2 = 2$ ואז $(1-\zeta_l)(i+\alpha(1-\zeta_l)) = 2$ כלומר $1-\zeta_l$ מחלק את 2 לכן l מחלק את 2, וזה לא ייתכן כי $2/l$ רציונלי לא שלם ולכן לא שייך ל-D_l. מכאן שהסימן הוא פלוס, כלומר קיים α כך ש-$i(1-\zeta_l) = \alpha(1-\zeta_l)^2$, ומכאן $i = \alpha(1-\zeta_l)$ כלומר $1-\zeta_l$ מחלק את i ולכן גם l מחלק אותו. מכאן ש-$\zeta_l^i = 1$ כנדרש. □

טענה 3.5.12. *אם $a \in D_l$ פרימרי ו-B אידאל שזר ל-(l) שעבורו NB זר ל-(a) אז*

$$(a/NB)_l = (NB/a)_l$$

הוכחה. $N(a)$ שייך ל-(a) כלומר מחלק את a, לכן $N(a), NB$ זרים ולפי טענה 3.5.9 מספיק להראות ש-$(\varepsilon(a)/B)_l = 1$. מאחר ש-a פרימרי $\varepsilon(a) = \pm 1$ לפי הטענה הקודמת, ומאחר ש-l אי זוגי $(\pm 1)^l = \pm 1$, כלומר $x^l = \varepsilon(a)(B)$ פתירה ולכן הסימן הוא אכן 1. □

כעת נוכל לסיים את הוכחת חוק ההדדיות של אייזנשטיין. יהי $p \in \mathbb{Z}$ שלם שאינו l ושזר ל-α ב-D_l. יהי P אידאל ראשוני שמכיל את p. אז $NP = p^f$. לפי הטענה הקודמת

$$(\alpha/p)_l^f = (p/\alpha)_l^f$$

מאחר ש-f מחלק את $l-1 = [\mathbb{Q}(\zeta_l) : \mathbb{Q}]$ הוא זר ל-l, ולכן מכך שסימני השארית הם שורשי יחידה $(\alpha/p)_l = (p/\alpha)_l$. מכפליות נקבל ש-$(\alpha/a)_l = (a/\alpha)_l$ לכל $a \in \mathbb{Z}$ שזר ל-α, l, כנדרש.

3.6 יישומים

משפט 3.6.1. *יהיו $l \nmid a$ שלמים כך ש-l ראשוני אי זוגי. אם כמעט לכל ראשוני p המשוואה $x^l = a(p)$ פתירה, אז קיים b כך ש-$b^l = a$.*

הוכחה. נניח שאין b כזה. נרשום פירוק לראשוניים $aD_l = P_1^{a_1} \dots P_n^{a_n}$. נרשום $P_i \cap \mathbb{Z} = p_i\mathbb{Z}$. אז $p_i \neq l$ כי l לא מחלק את a, לכן לפי טענה 2.2.6 אינדקס ההסתעפות של P_i הוא 1. מכאן ש-$\mathrm{ord}_{p_i} a = \mathrm{ord}_{P_i} a = a_i$, כשהסדר הראשון הוא ב-$\mathbb{Z}$ והשני ב-D_l. אם l מחלק את a_i לכל i נקבל ש-a הוא חזקה l-ית ב-$\mathbb{Z}$. אחרת נניח ש-l לא מחלק את a_n.
תהי $S = \{Q_1, \dots, Q_k\}$ קבוצה סופית של ראשוניים Q_i ששונים מה-P_i ומ-$(1-\zeta_l)$. יהי α שעבורו $(\alpha/P_n)_l = \zeta_l$. לפי משפט 1.1.10 קיים $t \in D_l$ שעבורו $t = 1(Q_i), t = 1(l), t = 1(P_j)$ ל-$1 \leq j \leq n-1$ ו-$t = \alpha(P_n)$. מאחר ש-$t = 1(l)$ הוא פרימרי. מכאן לפי חוק ההדדיות ש

$$(a/t)_l = (t/a)_l = \prod (t/P_i)^{a_i} = \zeta_l^{a_n} \neq 1$$

מצד שני נרשום פירוק לראשוניים $(t) = R_1 \dots R_m$. אז

$$(a/t)_l = \prod_j (a/R_j)_l$$

ולכן עבור j כלשהו $(a/R_j)_l \neq 1$, כלומר המשוואה מהניסוח לא פתירה עבור R_j. מהשקילויות ש-t מקיים נובע ש-$R_j \notin \{Q_1, \dots, Q_k, (1-\zeta_l), P_1, \dots, P_n\}$. נסמן $Q(S) = R_j$.
כעת עבור $S_1 = \varnothing$ נקבל $Q(S_1)$ ראשוני שעבורו $x^l = a(Q(S_1))$ לא פתירה. עבור

$$S_2 = S_1 \cup \{Q(S_1)\}$$

נקבל ראשוני שונה מהקודם $Q(S_2)$ שעבורו $x^l = a(Q(S_2))$ לא פתירה. נמשיך בדרך הזאת ונקבל אינסוף ראשוניים Q עבורם המשוואה לא פתירה. לכל Q כזה נרשום $Q \cap \mathbb{Z} = q\mathbb{Z}$, אז $x^l = a(q)$ לא פתירה ויש אינסוף q כאלה כי כל ראשוני שלם מוכל במספר סופי של אידאלים ראשוניים. $\square$

משפט 3.6.2. *אם $x^l + y^l + z^l = 0$ פתירה בשלמים שונים מ-0 ואם l לא מחלק את xyz אז $2^{l-1} = 1(l^2)$.*

נסיק את המשפט הזה מהמשפט הבא:

משפט 3.6.3. *אם x, y, z שלמים שונים מ-0 וזרים בזוגות שעבורם $x^l + y^l + z^l = 0$ ו-l לא מחלק את yz אז לכל ראשוני $p|y$ מתקיים $p^{l-1} = 1(l^2)$.*

ההנחה ש-x, y, z זרים בזוגות לא מגבילה את הכלליות. אכן אם למשל x, y לא זרים נסמן ב-d את הגממ שלהם. מאחר ש-$z^l = -(x^l + y^l)$ ו-x^l, y^l מתחלקים ב-d^l גם z^l מתחלק ב-d^l, לכן z מתחלק ב-d ומתקיים $(x/d)^l + (y/d)^l + (z/d)^l = 0$, ו-$x/d, y/d$ זרים.
משפט 3.6.2 נובע ממשפט 3.6.3 כי אם $x^l + y^l + z^l = 0$ לא ייתכן ששלושתם אי זוגיים, לכן מכך ש-l לא מחלק את xyz נוכל להניח ש-$2|y$ ולפי המשפט $2^{l-1} = 1(l^2)$.
כעת נוכיח את המשפט. נסמן $\zeta = \zeta_l$. מתקיים

$$(x+y)(x+\zeta y) \dots (x + \zeta^{l-1} y) = x^l + y^l = (-z)^l$$

למה 3.6.4. *אם $0 \le i, j < l$ ו-$i \neq j$ אז $x + \zeta^i y, x + \zeta^j y$ זרים ב-D_l.*

הוכחה. יהי A אידאל שמכיל את שני האיברים. אז $(\zeta^j - \zeta^i)x, (\zeta^j - \zeta^i)y \in A$ מאחר ש-x, y זרים יש u, v כך ש-$ux + vy = 1$, לכן $(\zeta^j - \zeta^i)xu + (\zeta^j - \zeta^i)yv = \zeta^j - \zeta^i$ ומכאן ש-$\zeta^j - \zeta^i \in A$. נסמן $m = i - j$, אז $\zeta^m \neq 1$. מאחר ש-$\zeta^j - \zeta^i = \zeta^j(1 - \zeta^m)$ נקבל שגם $1 - \zeta^m \in A$. מכיוון שהחבורה הנוצרת ע"י ζ היא מסדר l והוא ראשוני כל איבר שונה מ-1 בה הוא יוצר שלה, ולכן $\zeta = \zeta^{mk}$ עבור k טבעי. מכאן ש-$\lambda = 1 - \zeta = (1 - \zeta^m)(1 + \zeta^m + \zeta^{2m} + \cdots + \zeta^{(k-1)m}) \in A$. מאחר ש-$(\lambda)$ מקסימלי $A = (\lambda)$ או $A = D_l$. במקרה הראשון מהשוויון שציינו לפני הלמה נקבל ש-$z \in (\lambda)$ ומכאן $l|z$ בסתירה להנחה. לכן $A = D_l$ כלומר האיברים זרים. □

מהלמה נקבל שהאידאלים $(x + \zeta^i y)$ הם חזקות lית, מאחר שמכפלתם היא $(-z)^l$.
נביט ב-$\alpha = (x+y)^{l-2}(x+\zeta y)$. האידאל שהוא יוצר הוא חזקה lית. נסמן $u = (x+y)^{l-2}y$. נשים לב ש-$x + \zeta y = x + y - y\lambda$, לכן $\alpha = (x + y)^{l-1} - \lambda u$. כעת $x^l + y^l + z^l = x + y + z(l)$, כלומר $x + y + z$ מתחלק ב-l. אם l מחלק את $x + y$ נקבל שהוא מחלק את z בסתירה להנחה, לכן הוא לא מחלק את $x + y$ ומכאן ש-$(x + y)^{l-1} = 1(l)$. מכאן ש $\alpha = 1 - u\lambda(\lambda^2)$.
מתקיים

$$\zeta^{-u}\alpha = (1 - \lambda)^{-u}\alpha = (1 + u\lambda)(1 - u\lambda) = 1(\lambda^2)$$

לכן ζ^{-u} פרימרי. לפי חוק ההדדיות ומאחר ש-$(\alpha) = (\zeta^{-u}\alpha)$ הוא חזקה lית

$$1 = (p/\zeta^{-u}\alpha)_l = (\zeta^{-u}\alpha/p)_l = (\zeta/p)_l^{-u}(\alpha/p)_l$$

מכיוון ש-$p|y$ מתקיים $\alpha = (x + y)^{l-1}(p)$. לכן שוב לפי חוק ההדדיות ומכך ש-$(x + y)$ חזקה lית

$$(\alpha/p)_l = ((x + y)^{l-1}/p)_l = (p/(x + y)^{l-1})_l = 1$$

ולכן נקבל ש-$(\zeta/p)_l^u = 1$.
נרשום פירוק לראשוניים $pD_l = P_1 \dots P_g$. אז $NP_i = p^f$ ואינדקס ההסתעפות e הוא 1 לפי טענה 2.2.6. מכאן ש-$gf = l - 1$. לפי טענה 3.2.4

$$(\zeta/p)_l = \prod_i (\zeta/P_i)_l = \prod_i \zeta^{\frac{p^f - 1}{l}} = \zeta^{g(p^f - 1)/l}$$

מכאן ומכך ש-$(\zeta_p)_l^u = 1$ נקבל ש

$$ug\frac{p^f - 1}{l} = 0(l\mathbb{Z})$$

מאחר ש-$g|l - 1$ l לא מחלק את g. בנוסף l לא מחלק את u כי הוא לא מחלק את y ואת $x + y$. מכאן שהוא מחלק את $\frac{p^f - 1}{l}$, כלומר $p^f = 1(l^2)$. מכאן ומכך ש-f מחלק את $l - 1$ נקבל את תוצאת המשפט.