TEL AVIV UNIVERSITY אוניברסיטת תל-אביב
RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES
SCHOOL OF MATHEMATICAL SCIENCES
הפקולטה למדעים מדויקים ע"ש ריימונד ובברלי סאקלר
בית הספר למדעי המתמטיקה

פונקציות אלגבריות של משתנה אחד

מערכי שעור

תשפ"א

נערך על ידי

דן הרן

עדכון אחרון: 1.8.2021

תוכן העניינים

ספרות מומלצת

- A. Deuring, *Lectures on the theory of algebraic functions of one variable*, Springer 1973
- C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, American Mathematical Society 1951
- H. Stichtenoth, *Algebraic function fields and codes*, 2nd edition, Graduate Texts in Mathematics 274, Springer 2008

מבוא

בקורס נחקור בעיקר משוואה מהצורה $f(X,Y)=0$ ("עקום אלגברי") באשר f פולינום אי פריק לחלוטין מעל שדה K כלשהו. (אי פריק לחלוטין –פירושו שאינו מתפרק מעל הרחבה כלשהי של K; באופן שקול הוא אי פריק מעל הסגור האלגברי של K.) נתעניין בפתרונות של המשוואה הנ"ל ("אפסים של f"), אך גם בדברים אחרים, שקשורים במשוואה.

במקום לדבר על המשוואה, נדבר על שדות: למשוואה הנ"ל מתאימים את שדה המנות של החוג $K[X,Y]/(f)$, "שדה הפונקציות" של f.

קיימת תורה אלגברית של מיון של שדות כאלה (תורת רימן־רוך).

בנוסף לכך אנו רוצים ללמוד על מספר הפתרונות ("אפסים") של המשוואה הנ"ל:

השערת רימן לעקומים: *נסמן ב־ $\mathbb{F}_q$ את השדה בן q איברים. יהי $f \in \mathbb{F}_{q_0}[X,Y]$ אי פריק מעל $\tilde{\mathbb{F}}_{q_0}$. עבור הרחבה $\mathbb{F}_q$ של $\mathbb{F}_{q_0}$ נסמן ב־ N_q את מספר האפסים של f מעל $\mathbb{F}_q$. אזי*

$$|N_q(f)-(q+1)| \leq 2g\sqrt{q}$$

באשר g תלוי ב־ f, אך לא ב־ q.

השערה זו הוכחה על ידי André Weil בשנת 1949. יש גם הכללה של משפט זה (Lang-Weil), כאשר במקום פולינום בשני משתנים לוקחים יותר פולינומים ביותר משתנים.

כידוע, פונקציית זיתא של רימן הקלאסית מוגדרת כהמשכה אנליטית של

$$\zeta(s)=\sum_{n=0}^{\infty}\frac{1}{n^s}, \qquad s>1$$

למישור המרוכב. היא מתאפסת עבור $s=-2,-4,\dots$ ("האפסים הטריביאליים"). השערת רימן אומרת שכל האפסים האחרים של ζ נמצאים על הישר $\mathrm{Re}\ s=\frac{1}{2}$.

אנו נגדיר בהמשך פונקציית זיתא עבור עקומים אלגבריים, עבורה יש השערה דומה. היא שקולה להשערת רימן לעקומים.

הכללה של השערה זו ליריעות (במקום עקומים) הוכחה על ידי Pierre Deligne בשנת 1971. היא גם משפרת את ההערכה על מספר האפסים.

1. חבורות סדורות, הערכות, חוגי הערכה ואתרים

הגדרה 1.1: חבורה אבלית Γ (עם פעולה: $+$) עם יחס סדר $\leq$ מלא (=טוטאלי: לכל $\alpha,\beta\in\Gamma$ מתקיים $\alpha\leq\beta$ או $\beta\leq\alpha$) תיקרא **חבורה סדורה** אם יחס הסדר שומר חיבור, כלומר, $\alpha\leq\beta \Leftarrow \alpha+\gamma\leq\beta+\gamma$ לכל $\alpha,\beta,\gamma\in\Gamma$.
נכתוב $\alpha<\beta$ אם $\alpha\leq\beta$ אבל $\alpha\neq\beta$. ∎

דוגמאות 1.2: (א) $\mathbb{Z}$, $\mathbb{R}$, עם הסדר הרגיל.

(ב) $\mathbb{Z}\oplus\mathbb{Z}$ עם הסדר הלקסיקוגרפי: $(\alpha_1,\alpha_2)\leq(\beta_1,\beta_2)$ אם $\alpha_1<\beta_1$ או $\alpha_1=\beta_1, \alpha_2\leq\beta_2$.

(ג) באופן כללי יותר, אם Γ_1,Γ_2 חבורות סדורות אז $\Gamma_1\oplus\Gamma_2$ עם הסדר הלקסיקוגרפי היא חבורה סדורה.

תרגיל 1.3: *תהי Γ חבורה סדורה. (א) יהי $\gamma\in\Gamma$. אם $\gamma\geq 0$ אז $-\gamma\leq 0$.*

(ב) *$\Gamma_+ := \{\gamma\in\Gamma|\ \gamma\geq 0\}$ היא תת־מונואיד (תת־קבוצה סגורה תחת החיבור ומכילה 0) של Γ.*

(ג) $\Gamma=-\Gamma_+\cup\Gamma_+$, $\{0\}=-\Gamma_+\cap\Gamma_+$.

(ד) *תהי Δ חבורה אבלית ותהי Δ_+ תת מונואיד שלה כך שמתקיים $\Delta=-\Delta_+\cup\Delta_+$, $-\Delta_+\cap\Delta_+=\{0\}$. נגדיר יחס $\leq$ על Δ על ידי: $\alpha\leq\beta$ אם $\beta-\alpha\in\Delta_+$. אז Δ חבורה סדורה ביחס ל־$\leq$.*

תרגיל 1.4: *תהי Γ חבורה סדורה. אז לכל $n\in\mathbb{N}$ ההעתקה $\gamma\mapsto n\gamma$ היא מונומורפיזם שומר סדר $\varphi_n\colon\Gamma\to\Gamma$.*

הוכחה: כיוון ש־Γ אבלית, φ_n הוא הומומורפיזם של חבורות.
נראה שאם $\alpha\in\operatorname{Ker}\varphi_n$ אז $\alpha=0$. בלי הגבלת הכלליות $\alpha\geq 0$ (אחרת נחליף α ב־$-\alpha$). אז, באינדוקציה על n, מתקיים $\alpha\leq n\alpha$. לכן $0\leq\alpha\leq n\alpha=0$ ומכאן $\alpha=0$.
כעת נראה, באינדוקציה על n, שאם $\alpha\leq\beta$ אז $n\alpha\leq n\beta$. לפי הנחת האינדוקציה $(n-1)\alpha\leq(n-1)\beta$. לכן

$$n\alpha=(n-1)\alpha+\alpha\leq(n-1)\beta+\alpha\leq(n-1)\beta+\beta=n\beta.$$ ∎

מסקנה 1.5: *תהי Γ חבורה סדורה. כל $0\neq\gamma\in\Gamma$ מסדר אינסופי. בפרט, Γ אינסופית או $\Gamma=\{0\}$.*

הוכחה: נניח כי γ מסדר $n<\infty$. אז $\gamma\in\operatorname{Ker}\varphi_n$. לפי תרגיל 1.4, $\operatorname{Ker}\varphi_n=\{0\}$. לכן $\gamma=0$.

לפעמים נוסיף לחבורה סדורה Γ איבר נוסף ∞ ונרחיב את $+,\leq$ על הקבוצה (לא חבורה!) $\Gamma\cup\{\infty\}$ על ידי $\infty=\infty+\infty=\infty+\gamma=\gamma+\infty$, $\gamma<\infty$, לכל $\gamma\in\Gamma$.

הגדרה 1.6: **הערכה** (valuation) **על שדה** F היא העתקה $v\colon F^\times\to\Gamma$ לתוך חבורה סדורה Γ, המקיימת לכל $a,b\in F$

(א) $v(ab)=v(a)+v(b)$,

(ב) $v(a+b)\geq\min\big(v(a),v(b)\big)$

בתנאי שכל הביטויים מוגדרים (כלומר, $a,b\in F^\times$ ובתנאי (ב) גם $a+b\neq 0$). אבל:

אם נרחיב את v להעתקה $v\colon F \to \Gamma \uplus \{\infty\}$ על ידי

(ג) $v(a) = \infty \Leftrightarrow a = 0$.

אז (א), (ב) מתקיימים לכל $a, b \in F$ (ללא הגבלות).

להיפך, אם $v\colon F \to \Gamma \uplus \{\infty\}$ מקיימת (א), (ב), (ג) לכל $a, b \in F$ אז היא הערכה.

שתי הערכות v, v' של F נקראות **שקולות** אם $v'(a) \geq 0 \Leftrightarrow v(a) \geq 0$ לכל $a \in F^\times$.

דוגמאות 1.7: (1) עבור שדה כלשהו F וחבורה סדורה כלשהי Γ נגדיר $v\colon F^\times \to \Gamma$ על ידי של $v(a) = 0$ לכל a. זוהי **ההערכה הטריביאלית** על F.

(2) יהי p ראשוני. לכל איבר של $\mathbb{Q}^\times$ הצגה יחידה מהצורה $\frac{a}{b}p^n$, באשר $a, b \in \mathbb{Z} \setminus \{0\}$ זרים ל־p, $b > 0$, ו־$n \in \mathbb{Z}$. נגדיר $v(\frac{a}{b}p^n) = n$. אז $v\colon \mathbb{Q}^\times \to \mathbb{Z}$ הערכה; (הוכיחו!) נקראת **ההערכה ה־p־אדית**.

(3) יהי x טרנסצנדנטי מעל שדה F. תהי $w\colon F^\times \to \Gamma$ הערכה. תהי $\Gamma \oplus \mathbb{Z}$ (עם הסדר הלקסיקוגרפי) חבורה סדורה ונגדיר $v\colon F(x)^\times \to \Gamma \oplus \mathbb{Z}$ באופן הבא: אם $0 \neq f = \sum_i a_i x^i \in F[x]$, יהי $v(f) = \min_i \big(w(a_i), i\big)$, ועבור $0 \neq f, g \in F[x]$ נגדיר $v(f/g) = v(f) - v(g)$. אפשר להראות שההגדרה טובה ו־v הערכה. (תרגיל לא לגמרי טריביאלי, מסתמך על החומר בהמשך.) ∎

הערה 1.8: תהי $v\colon F \to \Gamma \uplus \{\infty\}$ הערכה ונניח כי $\Gamma \leq \mathbb{R}$. נבחר $0 < c < 1$ ממשי ונגדיר $|a| = c^{v(a)}$ לכל $a \in F$ (בפרט $|0| = c^\infty = 0$). אז $|ab| = |a| \cdot |b|$, $|a+b| \leq \max(|a|, |b|)$ ובפרט $|a+b| \leq |a| + |b|$.

כלומר, אם $\Gamma \leq \mathbb{R}$, הערכה היא מקרה פרטי של **ערך מוחלט**, (כתוב באופן חיבורי, לא כפלי). ∎

הערה 1.9: אם $v\colon F^\times \to \Gamma$ הערכה, אז $v(F^\times)$ תת חבורה סדורה של Γ, שנקראת **חבורת ההערכה של** v. אפשר להחליף את Γ בה ולכן להניח ש־v על. הערכה v נקראת **בדידה** אם $v(F^\times) \cong \mathbb{Z}$. ∎

טענה 1.10: *תהי* $v\colon F \to \Gamma \uplus \{\infty\}$ *הערכה. אז לכל* $a, b, a_1, \dots a_n \in F$

(א) $v(1) = 0$.

(ב) $v(-a) = v(a)$. *בפרט* $v(-1) = 0$.

(ג) *אם* $v(a) < v(b)$ *אז* $v(a+b) = v(a)$.

(ד) $v(\sum_{i=1}^n a_i) \geq \min(v(a_i))$.

(ה) *אם* $\sum_{i=1}^n a_i = 0$*, באשר* $n \geq 2$*, אז יש* $i \neq j$ *כך ש־* $v(a_i) = v(a_j)$.

הוכחה: (א) $v\colon F^\times \to \Gamma$ הוא הומומורפיזם חבורות, לכן מעביר איבר ניטרלי לאיבר ניטרלי.

(ב) $v(-a) = v(-1) + v(a)$, לכן די להוכיח כי $v(-1) = 0$. ואכן, $0 = v(1) = v(-1) + v(-1)$. לכן $v(-1)$ מסדר סופי (2 או 1). לפי מסקנה 1.5, $v(-1) = 0$.

(ג) $v(a+b) \geq \min\big(v(a), v(b)\big) = v(a)$. נניח בשלילה $v(a+b) > v(a)$. אז $v(a) = v(a+b-b) \geq \min\big(v(a+b), v(b)\big) > v(a)$, סתירה.

(ד) באינדוקציה על n.

(ה) נניח שלא. אז בלי הגבלת הכלליות $v(a_1) < v(a_2) < \cdots < v(a_n)$. באינדוקציה על n, לפי (ג), $v(\sum_{i=1}^n a_i) = v(a_1)$. אך $v(a_1) \neq \infty$, לכן $\sum_{i=1}^n a_i \neq 0$. סתירה. ∎

תרגיל 1.11: *יהי F תחום שלמות, יהי K שדה המנות שלו, ותהי $v\colon F \to \Gamma \cup \{\infty\}$ העתקה שמקיימת את התנאים (א),(ב), (ג) של הגדרה 1.6. אז v ניתנת להרחבה באופן יחיד להערכה $v\colon K \to \Gamma \cup \{\infty\}$.*

הגדרה 1.12: תחום שלמות R בעל שדה מנות F נקרא **חוג הערכה** אם לכל $a \in F^\times$ מתקיים: $a \in R$ או $a^{-1} \in R$. ∎

תרגיל 1.13: *תהי v הערכה על שדה F. אז $\mathcal{O}_v := \{a \in F |\ v(a) \geq 0\}$ הוא חוג הערכה בעל שדה מנות F; הוא נקרא **חוג ההערכה של** v. מתקיים $\mathcal{O}_v^\times = \{a \in F |\ v(a) = 0\}$. להערכות שקולות אותו חוג הערכה.*

למה 1.14: *יהי R חוג הערכה ויהי F שדה המנות שלו. אז*

(א) $R^\times = \{a \in R |\ a^{-1} \in R\}$.

(ב) *נסמן $\dot{R} = R \smallsetminus \{0\}$. אז $F^\times = \dot{R} \cup \dot{R}^{-1}$, $\dot{R} \cap \dot{R}^{-1} = R^\times$.*

(ג) $m = R \smallsetminus R^\times$ *הוא אידאל מרבי יחיד של R.*

הוכחה: (א), (ב) ברורים.

(ג) נראה ש־m אידאל.

יהיו $a \in m$, $r \in R$. אז $ra \in R$, אבל $ra \notin R^\times$, אחרת $a^{-1} = (ra)^{-1} r \in R$, סתירה; לכן $ra \in m$.

יהיו $a, b \in m$; צריך להוכיח $a + b \in m$. בה"כ $a, b \neq 0$. לפי ההנחה, $a/b \in R$ או $b/a \in R$. בה"כ $a/b \in R$. אז $1 + a/b \in R$. לכן לפי האמור לעיל $a + b = b(1 + a/b) \in m$.

כעת, m מרבי, כי כל איבר ב־$R \smallsetminus m$ הינו הפיך ב־R ולכן אינו שייך לאף אידאל נאות של R. הוא מרבי יחיד, כי כל אידאל נאות של R מוכל ב־$m = R \smallsetminus R^\times$. ∎

משפט 1.15: *ההעתקה $v \mapsto \mathcal{O}_v$ היא התאמה חח"ע בין מחלקות השקילות של ההערכות על שדה F לבין חוגי הערכה בעלי שדה המנות F.*

הוכחה: נגדיר העתקה הופכית.

יהי $F \subseteq R$ חוג הערכה ש־F שדה המנות שלו. נסמן $\dot{R} = R \smallsetminus \{0\}$. אז $\dot{R}, \dot{R}^{-1}$ תת מונואידים של החבורה הכפלית $F^\times$ ומתקיים $R^\times \subseteq \dot{R}, \dot{R}^{-1} \subseteq F^\times$. לפי למה 1.14, $F^\times / R^\times = \dot{R}/R^\times \cup \dot{R}^{-1}/R^\times$, $\dot{R}/R^\times \cap \dot{R}^{-1}/R^\times = R^\times/R^\times = \{1\}$. לפי תרגיל 1.3, $F^\times/R^\times$ חבורה סדורה (אמנם בכתיב כפלי, לא חיבורי).

תהי $w\colon F^\times \to F^\times/R^\times$ העתקת המנה. לפי הגדרת הסדר בתרגיל 1.3

$$w(a) \leq w(b) \Leftrightarrow \frac{w(b)}{w(a)} \in \dot{R}/R^\times \Leftrightarrow w(b/a) \in \dot{R}/R^\times \Leftrightarrow b/a \in \dot{R} \Leftrightarrow b/a \in R.$$

אז w הערכה: $w(ab)=w(a)w(b)$, כי w הומומורפיזם, ואם $w(a)\le w(b)$, כלומר, $b/a\in\dot R$, ו־$b\neq -a$, אז $(a+b)/a=1+b/a\in\dot R$, כלומר, $w(a+b)\ge w(a)=\min\big(w(a),w(b)\big)$.

לכן w הערכה על F. מתקיים $\mathcal{O}_w=\{a\in F|\ w(a)\ge 1=w(1)\}=\{a\in F|\ a\in R\}=R$.

אם $R=\mathcal{O}_v$, באשר v הערכה, אז w שקולה ל־v. אכן, $w(a)\ge 0\Leftrightarrow a\in R\Leftrightarrow v(a)\ge 0$.

לכן $w \mapsto R$ שהגדרנו לעיל הופכית ל־$v\mapsto\mathcal{O}_v$. ∎

יהי K שדה. נוסיף אליו איבר נוסף ∞ (אין קשר ל־∞ שהוספנו ל־Γ) ונרחיב את פעולות מ־K ל־$K\cup\{\infty\}$ באופן הבא: עבור $a\in K$, $b\in K^\times$

$$b/0=\infty\quad, a/\infty=0\quad, b\cdot\infty=\infty\cdot b=\infty\cdot\infty=\infty\quad, a\pm\infty=\infty\pm a=\infty.$$

ביטויים $\infty\pm\infty, 0\cdot\infty, \infty\cdot 0, 0/0, \infty/\infty$ אינם מוגדרים.

הגדרה 1.16: **אתר** (place) **משדה** F **לתוך שדה** K היא העתקה $\varphi\colon F\to K\cup\{\infty\}$ שמקיימת $\varphi(1)=1$ וכן

$$\varphi(ab)=\varphi(a)\varphi(b)\quad,\varphi(a+b)=\varphi(a)+\varphi(b), \tag{1}$$

לכל $a,b\in F$ עבורם אגף ימין מוגדר. שים לב שאם $\varphi(b)\neq 0,\infty$ אז גם $\varphi(a/b)=\varphi(a)/\varphi(b)$.

שני אתרים φ,φ' של שדה F נקראים **שקולים** אם $\varphi'(a)\neq\infty\Leftrightarrow\varphi(a)\neq\infty$ לכל $a\in F$. ∎

דוגמה 1.17: (א) יהי p ראשוני. נסמן $\mathbb{F}_p:=\mathbb{Z}/p\mathbb{Z}$. את העתקת המנה $\psi\colon\mathbb{Z}\to\mathbb{F}_p$ ניתן להרחיב לאתר $\varphi\colon\mathbb{Q}\to\mathbb{F}_p\cup\{\infty\}$: לכל איבר של $\mathbb{Q}$ הצגה יחידה מהצורה $\frac{a}{b}$, באשר $a,b\in\mathbb{Z}$, $b>0$, ו־a,b זרים או $a=0,b=1$. נגדיר $\varphi(\frac{a}{b})=\begin{cases}\frac{\psi(a)}{\psi(b)} & p\nmid b\\ \infty & p|b\end{cases}$. אז φ אתר.

(ב) אתר $\varphi\colon F\to K\cup\{\infty\}$ נקרא **טריביאלי** אם $\varphi(a)\neq\infty$ לכל $a\in F$. אז $\varphi\colon F\to K$ שיכון של שדות. להיפך, שיכון כזה הוא דוגמה לאתר טריביאלי. כל אתר טריביאלי שקול לזהות $F\to F$. ∎

למה 1.18: *יהי φ אתר על שדה F. אז*

(א) *$\varphi(0)=0$ ו־$\varphi(-a)=-\varphi(a)$ לכל $a\in F$ (כאשר $-\infty=\infty$).*

(ב) *$\bar F:=\varphi(F)\smallsetminus\{\infty\}$ הוא תת שדה של K. נקרא* **שדה השאריות** (residue field) **של** *φ.*

הוכחה: (א) $\varphi(1)=\varphi(1)+\varphi(0)$, (ושים לב שאגף ימין מוגדר, כי $\varphi(1)=1\neq\infty$, ולכן הוא שונה מ־∞) לכן $\varphi(0)=0$.

ואילו $\varphi(a)+\varphi(-a)=\varphi(0)=0$, אם אגף שמאל מוגדר, לכן $\varphi(-a)=-\varphi(a)$.

(אם $\varphi(a)=\infty$ אז $\varphi(-a)=\infty=-\infty$.)

(ב) לפי (1), $\bar F$ סגור תחת החיבור והכפל. לפי (א) הוא סגור תחת הנגדי. אם $c:=\varphi(a)\neq 0,\infty$ אז $\varphi(a^{-1})\neq\infty$, כי $\varphi(a)\varphi(a^{-1})=\varphi(1)=1$ ואילו $c\cdot\infty=\infty$. לכן $c^{-1}=\varphi(a^{-1})\in\bar F$. ∎

תרגיל 1.19: *יהי φ אתר על שדה F. אז $\mathcal{O}_\varphi := \{a \in F |\ \varphi(a) \neq \infty\}$ הוא חוג הערכה בעל שדה מנות F; הוא נקרא* **חוג ההערכה של** *φ. מתקיים $\mathcal{O}_\varphi^\times = \{a \in F |\ \varphi(a) \neq \infty, 0\}$. לאתרים שקולים אותו חוג הערכה.*

משפט 1.20: *ההעתקה $\varphi \mapsto \mathcal{O}_\varphi$ היא התאמה חח"ע בין מחלקות השקילות של האתרים על שדה F לבין חוגי הערכה בעלי שדה המנות F.*

הוכחה: נגדיר העתקה הופכית. יהי $R \subseteq F$ חוג הערכה ש־F שדה המנות שלו ויהי m האידאל המרבי של R. אז $K := R/m$ שדה. נרחיב את העתקת המנה $\psi\colon R \to K$ להעתקה $\psi\colon F \to K \cup \{\infty\}$ על ידי $\psi(a) = \infty$ לכל $a \in F \smallsetminus R$. אז ψ אתר.

אכן, יהיו $a, b \in F$. משוואות (1) ודאי מתקיימות, אם $\psi(a), \psi(b) \neq \infty$, כלומר, $a, b \in R$.

נניח $\psi(a) \neq \infty, \psi(b) = \infty$, כלומר, $a \in R, b \notin R$. אז $a + b \notin R$ (אחרת $b = (a+b) - a \in R$, סתירה), לכן $\psi(a+b) = \infty = \psi(a) + \psi(b)$. אם גם $\psi(a) \neq 0$, כלומר, $a \in R \smallsetminus m = R^\times$, אז $ab \notin R$ (אחרת $b = (ab)a^{-1} \in R$, סתירה), לכן $\psi(ab) = \infty = \psi(a)\psi(b)$.

נניח $\psi(a) = \psi(b) = \infty$, כלומר $a, b \notin R$. אז $a^{-1}, b^{-1} \in R$. לכן $ab \notin R$ (אחרת $b = a^{-1}(ab) \in R$, סתירה), לכן $\psi(ab) = \infty = \psi(a)\psi(b)$.

מתקיים $\mathcal{O}_\psi = \{a \in F |\ \psi(a) \neq \infty\} = \{a \in F |\ a \in R\} = R$.

אם $R = \mathcal{O}_\varphi$, באשר φ אתר, אז ψ שקול ל־φ, כי $\varphi(a) \neq \infty \Leftrightarrow a \in R \Leftrightarrow \psi(a) \neq \infty$.

לכן ההעתקה $R \mapsto \psi$ שהגדרנו לעיל הופכית להעתקה $\psi \mapsto \mathcal{O}_\psi$. ∎

ההגדרה של שקילות של הערכות ושל שקילות של אתרים אינה נראית טבעית. למעשה, צריך היה להגדיר את השקילויות אחרת. אך התרגיל הבא מראה שההגדרות שקולות לאלה שרשומות לעיל:

תרגיל 1.21: *הראו כי*

(א) *הערכות v, v' של שדה F שקולות אם ורק אם קיים איזומורפיזם חבורות שומר סדר $\lambda\colon v(F^\times) \to v'(F^\times)$ כך ש־$v' = \lambda \circ v$.*

(ב) *אתרים φ, φ' של שדה F שקולים אם ורק אם קיימת העתקה חד חד ערכית ועל $\lambda\colon \varphi(F) \to \varphi'(F)$ כך ש־$\lambda(\infty) = \infty$, $\lambda\colon \varphi(F) \smallsetminus \{\infty\} \to \varphi'(F) \smallsetminus \{\infty\}$ הוא איזומורפיזם של שדות, ו־$\varphi' = \lambda \circ \varphi$.*

$$\begin{tikzcd}
 & F \arrow[dl, "\varphi'"'] \arrow[dr, "\varphi"] & \\
\varphi(F) & & \varphi'(F) \\
\varphi(F) \smallsetminus \{\infty\} \arrow[u, hook] \arrow[rr, "\lambda"] & & \varphi'(F) \smallsetminus \{\infty\} \arrow[u, hook]
\end{tikzcd}$$

2. הערכות של שדות של פונקציות רציונליות

הגדרה 2.1: יהי K שדה ויהי t טרנסצנדנטי מעליו. אז $F = K(t) = \{\frac{f(t)}{g(t)} | \ f, g \in K[t], \ g \neq 0\}$ נקרא **שדה הפונקציות הרציונליות מעל K ב־t**.

עבור $u = \frac{f(t)}{g(t)} \in K(t)$ מגדירים $\deg u = \deg f - \deg g$.

זוהי הגדרה טובה: אם גם $u = \frac{f_0(t)}{g_0(t)} \in K(t)$, אז $f(t)g_0(t) = f_0(t)g(t)$ ולכן המעלות של שני האגפים שווים, כלומר, $\deg f + \deg g_0 = \deg f_0 + \deg g$. מכאן $\deg f - \deg g = \deg f_0 - \deg g_0$. ∎

יהי M שדה, $K \subseteq M$. איך נראה אתר $\varphi \colon F \to M \cup \{\infty\}$ שהינו זהות על K (ולכן ההערכה המתאימה לו היא טריביאלית על K)?

(א) נניח $\tau := \varphi(t) \neq \infty$. נסמן $\varphi_0 = \varphi|_{K[t]}$. אז $\varphi_0 \colon K[t] \to M$ הומומורפיזם חוגים שומר K. אם $\operatorname{Ker} \varphi_0 = \{0\}$, אז φ_0 שיכון, ו־ $\varphi(f/g) = \varphi_0(f)/\varphi_0(g) \neq \infty$ לכל $f/g \in K(t)$. לכן אז φ אתר טריביאלי.

אחרת $\operatorname{Ker} \varphi_0 \neq \{0\}$. כיוון ש־$\operatorname{Ker} \varphi_0$ אידאל ראשוני (כי תמונת φ מוכלת בשדה ולכן היא תחום שלמות) בחוג ראשי, $\operatorname{Ker} \varphi_0 = (p)$, באשר $p \in K[t]$ אי פריק מתוקן. נשים לב ש־τ הוא שורש של p ב־M. לכל $u \in F^\times$ יש הצגה

$$u = p^m \frac{f}{g} \tag{1}$$

באשר $f, g \in K[t] \smallsetminus \{0\}$, זרים, זרים ל־$p$, ו־$m \in \mathbb{Z}$ יחיד. אז בהכרח

$$\varphi(u) = \begin{cases} \frac{f(\tau)}{g(\tau)} & m = 0 \\ 0 & m > 0 \\ \infty & m < 0 \end{cases}. \tag{2}$$

מכאן שחוג ההערכה של φ הוא $\mathcal{O}_p = \{f/g | \ f, g \in K[t], \ p \nmid g\}$.

בדומה לדוגמה 1.7(2), $v_p(u) = m$, באשר m נתון ב־(1), מגדיר הערכה על F שחוג ההערכה שלה הוא $\mathcal{O}_p$. לכן v_p ההערכה המתאימה ל־φ. היא נקראת **הערכה p־אדית** על $K(t)$. אם $p \neq q$ אי פריקים, אז $v_p(1/p) = -1, \ v_q(1/p) = 0$, לכן v_p, v_q אינן שקולות.

לכן: קיימת התאמה חח"ע בין הפולינומים האי פריקים המתוקנים ב־$K[t]$ לבין מחלקות השקילות של האתרים של F שהינם זהות על K וסופיים על t.

(ב) נניח $\varphi(t) = \infty$. אז $\varphi(t^{-1}) = 0$. לכל $u \in F^\times$ יש הצגה

$$u = \frac{a_k t^k + a_{k-1} t^{k-1} + \cdots + a_0}{b_l t^l + a_{l-1} t^{l-1} + \cdots + b_0} = t^{k-l} \frac{a_k + a_{k-1} t^{-1} + \cdots + a_0 t^{-k}}{b_l + a_{l-1} t^{-1} + \cdots + b_0 t^{-l}} \tag{3}$$

באשר $a_i, b_j \in K,\ a_k, b_l \neq 0$. אז φ מעתיק את המנה באגף ימין ל־$\frac{a_k}{b_l}$, שהינו שונה מ־$0, \infty$. לכן

$$\varphi(u) = \begin{cases} \frac{a_k}{b_l} & k = l \\ 0 & k < l \\ \infty & k > l \end{cases} \tag{4}$$

מכאן שחוג ההערכה של φ הוא

$$\mathcal{O}_p = \{f/g|\ f, g \in K[t],\ \deg f \leq \deg g\} = \{u \in K(t)|\ \deg u \leq 0\}.$$

קל לראות שההגדרה $v_\infty(u) := -\deg u$ נותנת הערכה על F ו־$\mathcal{O}_v = \mathcal{O}_p$. לכן v_∞ מתאימה ל־φ.

נסכם את הדיון:

משפט 2.2: *כל ההערכות השונות של שדה הפונקציות הרציונליות $K(t)$ שהינן טריביאליות על K ואינן טריביאליות הן v_p, באשר $p \in K[t]$ אי פריק מתוקן (נתונות על ידי $(1), (2)$) או v_∞ (נתונה על ידי $(3), (4)$). בפרט כולן בדידות.*

באופן דומה למשפט הקודם:

תרגיל 2.2: *הוכח שההערכות ה־p־אדיות ($p \in \mathbb{N}$ ראשוני) הן הכל ההערכות הלא טריביאליות על $\mathbb{Q}$.*

3. הרחבת אתרים

משפט 3.1: *יהי R תת חוג של שדה F. יהי L שדה סגור אלגברית ויהי $\varphi\colon R\to L$ הומומורפיזם חוגים, $\varphi(1)=1$. נניח ש־φ אינו ניתן להרחבה להומומורפיזם חוגים $\varphi\colon R'\to L$ באשר $R\subsetneq R'\subseteq F$. אז R חוג הערכה בעל שדה מנות F ו־$\operatorname{Ker}\varphi$ האידאל המרבי היחיד של R.*

הוכחה: מתקיים $\varphi(1)\neq 0$, לכן $P:=\operatorname{Ker}\varphi\neq R$.

טענה 1: *P האידאל המרבי היחיד של R.* אכן, יהי

$$R'=\{\frac{r}{s}|\ r,s\in R,\ \varphi(s)\neq 0\}.$$

אז $R\subseteq R'\subseteq F$ ו־R' הוא חוג. ניתן להרחיב את φ על R' על ידי

$$\varphi(\frac{r}{s})=\frac{\varphi(r)}{\varphi(s)}.$$

(שים לב שהגדרה זו אינה תלויה ב־r,s אלא רק ב־$\frac{r}{s}$.) לכן, לפי ההנחה, $R=R'$. בפרט, אם $s\in R$, $\varphi(s)\neq 0$ אז $\frac{1}{s}\in R$. כלומר, $R\smallsetminus P\subseteq R^\times$. לכן $P\supseteq R\smallsetminus R^\times$. ההכלה ההפוכה נכונה לכל אידאל נאות, לכן $P=R\smallsetminus R^\times$. בכך הוכחה הטענה (שהרי כל אידאל נאות של R מוכל בקבוצה $R\smallsetminus R^\times$ והראינו שהיא אידאל.)

נשים גם לב ש־$K:=\varphi(R)\cong R/P$, וכיוון ש־P מרבי, K הוא שדה (תת שדה של L).

טענה 2: *יהי $z\in F^\times$. אז φ ניתן להרחבה ל־$R[z]$ או ל־$R[z^{-1}]$.* תחילה נרחיב את האפימורפיזם $\varphi\colon R\to K$ לאפימורפיזם של חוגי הפולינומים $\tilde{\varphi}\colon R[X]\to K[X]$ על ידי $\sum_i a_iX^i\mapsto\sum_i\varphi(a_i)X^i$. נרצה לבחור $\alpha\in L$ מתאים ולהגדיר אפימורפיזם־K $\lambda'\colon K[X]\to K[\alpha]\subseteq L$ על ידי $X\mapsto\alpha$. קיים תרשים חילופי

$$\begin{tikzcd}
R[X] \arrow[rrr, two heads, "\tilde{\varphi}"] \arrow[dr, "\lambda"] & & & K[X] \arrow[dl, "\lambda'"'] \\
& R[z] \arrow[r, dashed, "\psi"] & K[\alpha] & \\
R \arrow[uu] \arrow[ur] \arrow[rrr, two heads, "\varphi"'] & & & K \arrow[uu] \arrow[ul]
\end{tikzcd}$$

בו λ היא ההצבה $X\mapsto z$, $\varphi,\tilde{\varphi},\lambda'$ כמו שמוסבר לעיל, ושאר ההעתקות (הלא מקווקוות) הן ההכלות.

יהי

$$I=\operatorname{Ker}\lambda=\{f\in R[X]|\ f(z)=0\}.$$

אם נבחר את α כך ש־$(\lambda' \circ \tilde{\varphi})(I) = 0$, אז לפי משפט האיזומורפיזם הראשון לחוגים קיים אפימורפיזם $\psi\colon R[z] \to K[\alpha]$ כך שהטרפז העליון בתרשים חילופי. מהחילופיות של המלבן נובע בקלות שגם הטרפז התחתון חילופי, כלומר, ψ מרחיב את φ.

בגלל ש־$\tilde{\varphi}\colon R[X] \to K[X]$ הינו על, $\tilde{\varphi}(I)$ הואי אידאל ב־$K[X]$.

נבדיל בין כמה מקרים:

(א) $\tilde{\varphi}(I) = 0$. אז נבחר $\alpha \in L$ כלשהו, והתנאי $\lambda'(\tilde{\varphi}(I)) = 0$ מתקיים.

(ב) $\tilde{\varphi}(I) \neq 0, K[X]$. אז יש $f \in K[X]$ מתוקן כך ש־$\tilde{\varphi}(I) = (f)$. נבחר שורש כלשהו α של f ב־L. אז $\lambda'(f) = 0$, לכן $\lambda'(\tilde{\varphi}(I)) = 0$.

(ג) אחד משני המקרים הקודמים מתקיים עבור z^{-1} במקום z. אז נוכל להרחיב את φ ל־$R[z^{-1}] \to L$.

(ד) אחרת $\tilde{\varphi}(I) = K[X]$ ושוויון דומה נכון עם z^{-1} במקום z. אז יש $f, g \in R[X]$ כך ש־

$$f(z) = 0, \quad \tilde{\varphi}(f) = 1, \qquad g(z^{-1}) = 0, \quad \tilde{\varphi}(g) = 1 \tag{1}$$

כיוון ש־$\tilde{\varphi}(f) = 1$, $f \neq 0$; כיוון ש־$f(z) = 0$, אפילו $\deg f \geq 1$. באותו אופן $\deg g \geq 1$. נאמר

$$f = a_0 + a_1X + \cdots + a_nX^n, \quad g = b_0 + b_1X + \cdots + b_mX^m, \qquad a_n, b_m \neq 0, m, n \geq 1.$$

נבחר f, g ממעלות מזעריות אפשריות (כך שמתקיים (1)). בלי הגבלת הכלליות $m \leq n$. לפי (1), $\varphi(b_0) = 1$ ו־$\varphi(b_i) = 0$ עבור $i \geq 1$.

נגדיר $g_0 = b_0X^m + b_1X^{m-1} + \cdots + b_m$. אז $g_0(z) = z^m g(z^{-1}) = 0$. כמו כן $\tilde{\varphi}(g_0) = X^m$.

נחלק עם שארית את $b_0^n f$ ב־g_0 מעל R (זה אפשרי כי כל המקדמים של מחלק הם חזקה מתאימה של המקדם העליון של המחולק –ראה משפט 3.4 בסוף הפרק):

$$b_0^n f = g_0q + r, \qquad q, r \in R[X], \ \deg r < \deg g_0 = m \leq n. \tag{2}$$

נציב z ב־(2): נקבל $r(z) = 0$. נפעיל את $\tilde{\varphi}$ על (2):

$$1 = \varphi(b_0)^n \cdot 1 = X^m\tilde{\varphi}(q) + \tilde{\varphi}(r)$$

כיוון ש־$\deg \tilde{\varphi}(r) < m$, זה יתכן רק אם $\tilde{\varphi}(q) = 0$ ואז $\tilde{\varphi}(r) = 1$. לכן אפשר להחליף ב־(1) את f ב־r שהינו ממעלה נמוכה יותר, סתירה למזעריות $\deg f$. לכן מקרה זה לא יתכן.

סיום ההוכחה: לפי הטענה הקודמת, לכל $z \in F^\times$ מתקיים $z \in R$ או $z^{-1} \in R$. לכן R חוג הערכה. ∎

משפט 3.2: *יהי F שדה ויהי L שדה סגור אלגברית. יהיו R_0 תת חוג ו־F_0 תת שדה של F. אז*

(א) *כל הומומורפיזם $\varphi_0\colon R_0 \to L$ עם $\varphi_0(1) = 1$ ניתן להרחבה לאתר $\varphi\colon F \to L \cup \{\infty\}$.*

(ב) *כל אתר* $\varphi_0\colon F_0 \to L \cup \{\infty\}$ *ניתן להרחבה לאתר* $\varphi\colon F \to L \cup \{\infty\}$.

הוכחה: (א) הקבוצה $\Omega = \{(R, \varphi) |\ R_0 \subseteq R \subseteq F$ חוג, $\varphi\colon R \to L$ הומומורפיזם, $\varphi|_{R_0} = \varphi_0\}$ אינה ריקה כי $(R_0, \varphi_0) \in \Omega$. נגדיר עליה סדר חלקי: $(R, \varphi) \le (R', \varphi')$ אם $R \subseteq R'$ ו־φ' מרחיב את φ. אם $\{(R_\alpha, \varphi_\alpha)\}_\alpha$ שרשרת עולה ב־Ω אז $(\bigcup_\alpha R_\alpha, \bigcup_\alpha \varphi_\alpha) \in \Omega$ חסם מלעיל שלה. לפי הלמה של צורן יש $(R, \varphi) \in \Omega$ מרבי.

לפי משפט 3.1, R חוג הערכה בעל שדה מנות F ו־$m = \operatorname{Ker}\varphi$ האידאל המרבי שלו. נרחיב את φ להעתקה $\varphi\colon F \to L \cup \{\infty\}$ על ידי $\varphi(a) = \infty$ לכל $a \in F \smallsetminus R$. אז φ אתר. אכן, (זוהי חזרה על חלק מהוכחת משפט 1.20)

המשוואות

$$\varphi(ab) = \varphi(a)\varphi(b) \quad , \varphi(a+b) = \varphi(a) + \varphi(b) , \tag{3}$$

ודאי מתקיימות, אם $\varphi(a), \varphi(b) \neq \infty$, כלומר, $a, b \in R$.

נניח $\varphi(a) \neq \infty, \varphi(b) = \infty$, כלומר, $a \in R, b \notin R$. אז $a + b \notin R$ (אחרת $b = (a+b) - a \in R$, סתירה), לכן $\varphi(a+b) = \infty = \varphi(a) + \varphi(b)$. אם גם $\varphi(a) \neq 0$, כלומר, $a \in R \smallsetminus m = R^\times$, אז $ab \notin R$ (אחרת $b = (ab)a^{-1} \in R$, סתירה), לכן $\varphi(ab) = \infty = \varphi(a)\varphi(b)$.

נניח $\varphi(a) = \varphi(b) = \infty$, כלומר $a, b \notin R$. אז $a^{-1}, b^{-1} \in R$. לכן $ab \notin R$ (אחרת $b = a^{-1}(ab) \in R$, סתירה), לכן $\varphi(ab) = \infty = \varphi(a)\varphi(b)$. לכן (3) מתקיים.

(ב) לפי תרגיל 1.19, $R_0 := \{a \in F_0 |\ \varphi_0(a) \neq \infty\}$ הוא חוג הערכה. לפי (א) יש אתר $\varphi\colon F \to L \cup \{\infty\}$ אשר מרחיב את ההומומורפיזם $\varphi_0|_{R_0}$. אם $a \in F_0 \smallsetminus R_0$, כלומר, $\varphi_0(a) = \infty$, אז $\varphi_0(a^{-1}) = 0$ ובפרט $a^{-1} \in R_0$. לכן $\varphi(a^{-1}) = \varphi_0(a^{-1}) = 0$. מכאן $\varphi(a) = \infty$. בפרט $\varphi(a) = \varphi_0(a)$. לכן φ מרחיב את φ_0. ∎

מסקנה 3.3: *תהי* F/K *הרחבת שדות. יהי* $x \in F$ *טרנסצנדנטי מעל* K*. אז יש הערכות* v, v' *על* F *שהינן טריביאליות על* K *כך ש־*$v(x) > 0$ *ו־*$v'(x) < 0$.

הוכחה: לפי הדיון בפרק 2 האתר ה־x־אדי φ על $K(x)$ הינו זהות על K ומקיים $\varphi(x) = 0$. לפי משפט 3.2 ניתן להרחיב אותו לאתר של F. אז x נמצא באידאל המרבי של חוג ההערכה $\mathcal{O}_\varphi$, לכן ההערכה המתאימה v מקיימת $v(x) > 0$. היא טריביאלית על K, כי φ זהות על K.

באותו אופן יש הערכה v' כך ש־$v'(x^{-1}) > 0$. אז $v'(x) < 0$. ∎

משפט 3.4 (חילוק עם שארית): *יהי* R *חוג חילופי ויהיו* $f, g \in R[X]$,

$$g = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0 , \quad f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 .$$

פולינומים ב־$R[X]$. נניח ש־$m \geq 1$ ו־$b_m^k | a_k$ לכל $k \geq 1$. אזי קיימים $q, r \in R[X]$ כך ש־

$$f = gq + r, \qquad \deg r < \deg g = m.$$

אם b_m אינו מחלק אפס ב־R, אז q, r כאלה הם יחידים.

הוכחה: **קיום.** באינדוקציה על $\deg f$. אם $\deg f < m$ (ובפרט אם $f = 0$), ניקח $q = 0,\ r = f$.

נניח כעת כי $\deg f = n \geq m$ וטענת הקיום נכונה לכל הפולינומים ממעלה$< n$. אז לפי ההנחה יש $c_0 \in R$ כך ש־$a_n = b_m^n c_0$. נסמן $c = b_m^{n-1} c_0$. אז $b_m^{n-1} | c$ ו־$a_n = b_m c$. מכאן

$$f = g \cdot (cX^{n-m}) + f_1,$$

באשר

$$\begin{aligned} f_1 &= f - g \cdot (cX^{n-m}) \\ &= (a_n X^n + a_{n-1} X^{n-1} + \ldots + a_{n-m} X^{n-m} + a_{n-m-1} X^{n-m-1} + \ldots + a_0) \\ &- (b_m c X^n + b_{m-1} c X^{n-1} + \ldots + b_0 c X^{n-m}) \\ &= (a_n - b_m c) X^n + (a_{n-1} - b_{m-1} c) X^{n-1} + \ldots (a_{n-m} - b_0 c) X^{n-m} \\ &\qquad\qquad + a_{n-m-1} X^{n-m-1} + \ldots + a_0 \end{aligned}$$

כיוון ש־$a_n = b_m c$, מתקיים $\deg f_1 < n$. כיוון ש־$b_m^{n-1} | c$ ו־$b_m^k | a_k$, המקדם ה־k־י של f_1 מתחלק ב־b_m^k, לכל $k \geq 1$. לכן לפי הנחת האינדוקציה יש $q_1, r \in R[X]$ כך ש־

$$f_1 = gq_1 + r, \qquad \deg r < m.$$

לכן $f = g \cdot (cX^{n-m}) + gq_1 + r = gq + r$, באשר $q = cX^{n-m} + q_1$.

יחידות. נניח כי בנוסף ל־q, r יש גם $r_0, q_0 \in R[X]$ כך ש־

$$f = gq_0 + r_0, \qquad \deg r_0 < \deg g = m.$$

אז $g(q - q_0) = r_0 - r$. אם $q = q_0$ אז מכאן נובע שגם $r = r_0$. אם $q - q_0 \neq 0$, כלומר, $q - q_0 = c^\ell X^\ell + \ldots$, באשר $\ell \geq 0$, אז, כיוון ש־b_m אינו מחלק אפס, $g \cdot (q - q_0) = b_m c_\ell X^{m+\ell} + \ldots$ הינו פולינום ממעלה $m + \ell = \deg g + \deg q - q_0$. מכאן

$$\deg g \leq \deg g + \deg(q - q_0) = \deg g \cdot (q - q_0) = \deg(r - r_0) \leq \max(\deg r_0, \deg r) < \deg g,$$

סתירה. לכן $q = q_0$. ∎

4. הרחבות של שדות והערכות

יהי F שדה.

תהי $v\colon F^{\times} \to \Gamma$ הערכה, יהיו

$$\mathcal{O}_F = \{a \in F \mid v(a) \geq 0\}, \quad m_F = \{a \in F \mid v(a) > 0\}, \quad \varphi\colon F \to \bar{F} \cup \{\infty\}$$

חוג ההערכה שלה, האידאל המרבי שלו, ואתר מתאים לה, בהתאמה, באשר $\bar{F} = \mathcal{O}_F/m_F$ שדה השאריות, ו־φ מרחיב את העתקת המנה $\mathcal{O}_F \to \bar{F}$.

יהי E תת שדה של F (כלומר, F/E הרחבת שדות).

אז הצמצום $v\colon E^{\times} \to \Gamma$ הוא הערכה של E, חוג ההערכה שלה הוא $\mathcal{O}_E = E \cap \mathcal{O}_F$, האידאל המרבי שלו הוא $m_E = E \cap m_F$. הצמצום של φ ל־E הוא אתר של E. חוג ההערכה שלו הוא $E \cap \mathcal{O}_F = \mathcal{O}_E$, לכן $\varphi|_E$ מתאים ל־$v|_E$. שדה השאריות שלו $\bar{E} = \varphi(E) \smallsetminus \{\infty\} \cong \mathcal{O}_E/m_E$ הוא תת שדה של $\bar{F}$.

הגדרה 4.1: (א) $\big(v(F^{\times}) : v(E^{\times})\big)$ נקרא **אינדקס ההסתעפות** של F/E.

(ב) $[\bar{F} : \bar{E}]$ נקרא **אינדקס השארית** של F/E.

שניהם יכולים להיות מספרים טבעיים או ∞. ∎

משפט 4.2: $[\bar{F} : \bar{E}] \cdot \big(v(F^{\times}) : v(E^{\times})\big) \leq [F : E]$.

הוכחה: עבור $z \in \mathcal{O}_F$ נסמן $\bar{z} = \varphi(z) \in \bar{F}$.

יהיו $x_1, \dots, x_m \in \mathcal{O}_F$ כך ש־$\overline{x_1}, \dots, \overline{x_m} \in \bar{F}$ בלתי תלויים לינארית מעל $\bar{E}$. כמו כן יהיו $y_1, \dots, y_n \in F^{\times}$ כך ש־$v(y_1), \dots, v(y_n)$ מייצגים קוסטים שונים בחבורת המנה $v(F^{\times})/v(E^{\times})$. די להראות כי $\{x_i y_j\}_{i=1}^{m}\,_{j=1}^{n}$ בלתי תלויים לינארית מעל E.

כלומר, יהיו $a_{ij} \in E$ כך ש־$\sum_{i,j} a_{ij} x_i y_j = 0$; די להראות ש־$a_{ij} = 0$ לכל i, j.

נניח שזה לא כך. בלי הגבלת הכלליות לכל j יש i כך ש־$a_{ij} \neq 0$, אחרת נשמיט y_j מהסדרה $y_1, \dots, y_n$. נקבע j.

טענה: *יהיו* $x_1, \dots, x_m \in \mathcal{O}_F$ *כך ש־*$\overline{x_1}, \dots, \overline{x_m} \in \bar{F}$ *בלתי תלויים לינארית מעל* $\bar{E}$. *יהיו* $a_{ij} \in E$ *לא כולם אפס. אז* $v(\sum_{i=1}^{m} a_{ij} x_i) = \min_i v(a_{ij})$ *ובפרט* $v(\sum_{i=1}^{m} a_{ij} x_i) \in v(E^{\times})$.

אכן, יהי k כך ש־$v(a_{kj}) = \min_i v(a_{ij})$. לפי ההנחה $a_{kj} \neq 0$. אז

$$\min_i v(a_{ij}) - v(a_{kj}) = \min_i v\Big(\frac{a_{ij}}{a_{kj}}\Big), \qquad v\Big(\sum_{i=1}^{m} a_{ij} x_i\Big) - v\big(a_{kj}\big) = v\Big(\sum_{i=1}^{m} \frac{a_{ij}}{a_{kj}} x_i\Big),$$

לכן בטענה אפשר להחליף a_{ij} ב־$\frac{a_{ij}}{a_{kj}}$ ועל ידי כך להניח ש־$a_{kj} = 1$ ולכן $\min_i v(a_{ij}) = 0$. בפרט $a_{ij} \in \mathcal{O}_E$ לכל i ו־$a_{kj} \notin m_E$. כלומר, $\overline{a_{ij}} \in \bar{E}$ לכל i, אך לא כולם אפס, כי $\overline{a_{kj}} \neq 0$.

כיוון ש־$\overline{x_1}, \dots, \overline{x_m} \in \bar{F}$ בלתי תלויים לינארית מעל $\bar{E}$, $\overline{\sum_i a_{ij} x_i} = \sum_i \overline{a_{ij}}\,\overline{x_i} \neq 0$. לכן $\sum_i a_{ij} x_i \in \mathcal{O}_F \smallsetminus m_F$, כלומר, $v(\sum_i a_{ij} x_i) = 0$, כנטען.

סיום ההוכחה: מתקיים $\sum_{j=1}^{n}\Big(\sum_i a_{ij}x_i\Big)y_j = 0$. לפי הטענה $\sum_i a_{ij}x_i \neq 0$ (כי $v(0)=\infty$) ולפי ההנחה $y_j \neq 0$ לכל j. לכן $n \geq 2$. לפי טענה 1.10(ה) יש $j \neq l$ כך ש־

$$v\Big(\big(\sum_i a_{ij}x_i\big)y_j\Big) = v\Big(\big(\sum_i a_{il}x_i\big)y_l\Big),$$

כלומר

$$v\big(\sum_i a_{ij}x_i\big) + v(y_j) = v\big(\sum_i a_{il}x_i\big) + v(y_l),$$

ומכאן, לפי הטענה,

$$v(y_j) - v(y_l) = v\Big(\sum_i a_{il}x_i\Big) - v\Big(\sum_i a_{ij}x_i\Big) \in v(E^\times),$$

בסתירה לכך ש־$v(y_j), v(y_l)$ בקוסטים שונים מודולו $v(E^\times)$. ∎

מסקנה 4.3: *אינדקס ההסתעפות ואינדקס השארית קטנים או שווים למעלת ההרחבה. אם ההרחבה סופית, האינדקסים סופיים.*

למה 4.4: *תהיינה $\Delta \leq \Gamma$ חבורות סדורות. נניח $(\Gamma : \Delta) = n < \infty$. אם $\Delta \cong \mathbb{Z}$ אז $\Gamma \cong \mathbb{Z}$. אם $\Delta = \{0\}$ אז $\Gamma = \{0\}$.*

הוכחה: לפי תרגיל 1.4, ההעתקה $\gamma \mapsto n\gamma$ היא מונומורפיזם שומר סדר $\varphi_n\colon \Gamma \to \Gamma$.

יהי $\gamma \in \Gamma$. אז תמונתו ב־Γ/Δ היא מסדר שמחלק את $n = |\Gamma/\Delta|$, לכן $n\gamma \in \Delta$. לכן $\varphi_n(\Gamma) \leq \Delta$ ובפרט Γ איזומורפית לתת חבורה של Δ. לכן אם $\Delta = \{0\}$ אז $\Gamma = \{0\}$. אם $\Delta \cong \mathbb{Z}$, אז כל תת חבורה של Δ איזומורפית ל־$\mathbb{Z}$ או $\{0\}$. כיוון ש־Γ מכילה את Δ, היא אינה סופית ולכן $\Gamma \cong \mathbb{Z}$. ∎

מסקנה 4.5: *תהי F הרחבה סופית של שדה הפונקציות הרציונליות $E = K(t)$ מעל שדה K. אז כל הערכה לא טריביאלית v של F שהינה טריביאלית על K היא בדידה.*

הוכחה: לפי מסקנה 4.3, $\big(v(F^\times) : v(E^\times)\big) < \infty$. לפי למה 4.4, $v|_E$ אינה טריביאלית. לפי משפט 2.2, $v|E$ בדידה. לכן לפי למה 4.3, גם v בדידה. ∎

5. אי תלות של הערכות

בסעיף זה יהי F שדה ו־$v_1,\dots,v_n$ הערכות *לא טריביאליות* עליו. יהיו $\mathcal{O}_1,\dots,\mathcal{O}_n$ חוגי ההערכה שלהם, בהתאמה. אז $F \subsetneqq \mathcal{O}_i$ לכל i.

משפט 5.1: *אם* $\mathcal{O}_i \not\subseteq \mathcal{O}_1$ *לכל* $i \neq 1$ *אז יש* $x \in F$ *כך ש־*

$$v_2(x),\dots,v_n(x) < 0 \qquad v_1(x) \geq 0.$$

הוכחה: באינדוקציה על n. עבור $n=1$ מתקיים $v_1(1)=0$.

$n=2$: $\mathcal{O}_1 \not\subseteq \mathcal{O}_2$, לכן יש $x \in \mathcal{O}_1 \smallsetminus \mathcal{O}_2$. אז $v_1(x)\geq 0,\ v_2(x)<0$.

המקרה הכללי: לפי הנחת האינדוקציה יש $y \in F$ כך ש־$v_1(y)\geq 0, v_2(y),\dots,v_{n-1}(y)<0$. לפי המקרה $n=2$ קיים $z\in F$ כך ש־$v_1(z)\geq 0, v_n(z)<0$. נגדיר

$$x = y + z^m$$

באשר $m\in\mathbb{N}$ גדול מספיק, כך שלכל $i\geq 2$, עבורו $v_i(z)\neq 0$, מתקיים $v_i(z^m)=mv_i(z)\neq v_i(y)$. אי שוויון זה נכון גם אם $v_i(z)=0$, כי אז $2\leq i\leq n-1$ ולכן $v_i(y)<0=mv_i(z)$. כעת

(א) $v_1(x)\geq \min\big(v_1(y), mv_1(z)\big)\geq 0$.

(ב) אם $i\geq 2$ אז לפי טענה 1.10(ג) $v_i(x)=\min\big(v_i(y), mv_i(z)\big)<0$, כי $v_i(y)<0$ או $v_i(z)<0$.

∎

תרגיל 5.2: *התנאים הבאים שקולים זה לזה:*

(א) $\mathcal{O}_1\subseteq\mathcal{O}_2$.

(ב) $v_1(a)\geq 0 \Rightarrow v_2(a)\geq 0$, *לכל* $a\in F^\times$.

(ג) $v_1(a)\leq 0 \Rightarrow v_2(a)\leq 0$, *לכל* $a\in F^\times$.

(ד) $v_2(a)> 0 \Rightarrow v_1(a)> 0$, *לכל* $a\in F^\times$.

(ה) $v_2(a)< 0 \Rightarrow v_1(a)< 0$, *לכל* $a\in F^\times$.

הוכחה: (א) $\Leftrightarrow$ (ב): ההתאמה בין הערכות לחוגי הערכה. (ב) $\Leftrightarrow$ (ג): $a\leftrightarrow a^{-1}$. (ד) $\Leftrightarrow$ (ה): $a\leftrightarrow a^{-1}$. (ג) $\Leftrightarrow$(ד): על דרך השלילה. ∎

הגדרה 5.3: חבורה סדורה Γ נקראת **ארכימדית** אם לכל $0<\alpha\in\Gamma$, $\beta\in\Gamma$ קיים $m\in\mathbb{N}$ כך ש־$\beta<m\alpha$.

הגדרה שקולה: לכל $0>\alpha\in\Gamma$, $\beta\in\Gamma$ קיים $m\in\mathbb{N}$ כך ש־$\beta>m\alpha$.

הערכה תיקרא **ארכימדית** אם חבורת ההערכה שלה ארכימדית. ∎

למשל, $\mathbb{Z},\mathbb{R}$ חבורות ארכימדיות, $\mathbb{Z}\oplus\mathbb{Z}$ עם הסדר הלקסיקוגרפי אינה ארכימדית (כי $(1,0)>m(0,1)$ לכל $m\in\mathbb{N}$).

תרגיל 5.4: *כל חבורה סדורה ארכימדית ניתנת לשיכון שומר סדר לתוך $\mathbb{R}$.*

למה 5.5: *נניח כי v_1, v_2 ארכימדיות. אם $\mathcal{O}_1 \subseteq \mathcal{O}_2$ אז $\mathcal{O}_1 = \mathcal{O}_2$, כלומר, v_1, v_2 שקולות.*

הוכחה: יהי $a \in F^\times$ כך ש-$v_2(a) \geq 0$. לפי תרגיל 5.2 די לראות כי $v_1(a) \geq 0$.

יהי $b \in F^\times$ כך ש-$v_2(b) > 0$. אז לכל $m \in \mathbb{N}$ מתקיים $v_2(a^m b) = mv_2(a) + v_2(b) > 0$. לפי תרגיל 5.2, $v_1(a^m b) = mv_1(a) + v_1(b) > 0$, כלומר, $m\big(-v_1(a)\big) < v_1(b)$. כיוון ש-$v_1$ ארכימדית, זה יתכן רק אם $-v_1(a) \leq 0$, כלומר, $v_1(a) \geq 0$. ∎

אם ההערכות הן ארכימדיות, למה זאת מאפשרת לנו להניח הנחה חלשה יותר במשפט 5.1. אך אפשר גם לחזק את המסקנה שלו:

משפט 5.6: *אם $v_1, \ldots, v_n$ ארכימדיות ו-v_1 אינה שקולה ל-v_i לכל $i \neq 1$ אז יש $x \in F$ כך ש-*

$$v_1(x) > 0, \qquad v_2(x), \ldots, v_n(x) < 0.$$

הוכחה: לפי למה 5.5, $\mathcal{O}_1 \not\subseteq \mathcal{O}_i$ לכל $i \neq 1$. לפי משפט 5.1 יש $z \in F$ כך ש-

$$v_1(z) \geq 0, \qquad v_2(z), \ldots, v_n(z) < 0.$$

נבחר $y \in F^\times$ כך ש-$v_1(y) > 0$. יהי $m \in \mathbb{N}$ גדול מספיק. אז $x := z^m y$ מקיים את המבוקש, בגלל הארכימדיות של $v_2, \ldots, v_n$. ∎

למה 5.7: *אם $v_1, \ldots, v_n$ ארכימדיות ו-$\rho_1, \ldots, \rho_n$ איברים בחבורות ההערכה שלהם, בהתאמה, ו-v_1 אינה שקולה ל-v_i לכל $i \neq 1$ אז יש $x \in F$ כך ש-*

$$v_1(x-1) > \rho_1, \qquad v_i(x) > \rho_i, \quad i = 2, \ldots, n.$$

הוכחה: לפי משפט 5.6 יש $y \in F$ כך ש- $v_1(y) > 0, \quad v_2(y), \ldots, v_n(y) < 0$. אז לכל $m \in \mathbb{N}$

$$v_i(1+y^m) = \min\big(v_i(1), mv_i(y)\big) = \begin{cases} 0 & i = 1 \\ mv_i(y) & i \geq 2 \end{cases},$$

לכן אם נגדיר $x = \frac{1}{1+y^m}$, באשר $m \in \mathbb{N}$ גדול מספיק, אז

$$v_1(x-1) = v_1(-\frac{y^m}{1+y^m}) = mv_1(y) - 0 > \rho_1,$$
$$v_i(x) = -v_i(1+y^m) = -mv_i(y) > \rho_i, \quad i = 2, \ldots, m.$$
∎

למה 5.8: אם $v_1, \ldots, v_n$ *הערכות ארכימדיות לא שקולות (בזוגות),* $\rho_1, \ldots, \rho_n$ *איברים בחבורות ההערכה שלהם, בהתאמה, ו־* $a_1, \ldots, a_n \in F$*, אז יש* $x \in F$ *כך ש־* $v_i(x - a_i) > \rho_i$ *לכל* i.

הוכחה: אם $a_1 = \cdots = a_n = 0$, ניקח $x = 0$. אחרת נסמן $\tau_i = \min_j v_i(a_j) \in v_i(F^\times)$ לכל i. לפי למה 5.7, לכל j קיים $x_j \in F$ כך ש־

$$i \neq j \quad v_i(x_j) > \rho_i - \tau_i, \qquad v_j(x_j - 1) > \rho_j - \tau_j.$$

ובפרט $v_i(x_i - 1) > \rho_i - \tau_i$ לכל i. נגדיר $x = a_1x_1 + \cdots + a_nx_n$. אז, לכל i,

$$x - a_i = (x - a_ix_i) + (a_ix_i - a_i) = \sum_{j \neq i} a_jx_j + a_i(x_i - 1),$$

לכן, לכל i,

$$v_i(x - a_i) \geq \min\big(\{v_i(a_j) + v_i(x_j)\}_{j \neq i}, v_i(a_i) + v_i(x_i - 1)\big) \geq \tau_i + (\rho_i - \tau_i) = \rho_i.$$ ∎

משפט 5.9 (משפט הקירוב החלש): אם $v_1, \ldots, v_n$ *הערכות ארכימדיות לא שקולות (בזוגות),* $\rho_1, \ldots, \rho_n$ *איברים בחבורות ההערכה שלהם, בהתאמה, ו־* $a_1, \ldots, a_n \in F$*, אז יש* $x \in F$ *כך ש־* $v_i(x - a_i) = \rho_i$ *לכל* i.

הוכחה: לפי למה 5.8 יש $y \in F$ כך ש־$v_i(y - a_i) > \rho_i$ לכל i. לכל i נבחר $b_i \in F$ כך ש־ $v_i(b_i) = \rho_i$. שוב לפי למה 5.8 יש $z \in F$ כך ש־$v_i(z - b_i) > \rho_i$ לכל i. נגדיר $x = y + z$. אז $x - a_i = y + z - a_i = (y - a_i) + (z - b_i) + b_i$, לכן

$$v_i(x - a_i) = \min\big(v_i(y - a_i), v_i(z - b_i), v_i(b_i)\big) = \rho_i$$

לכל i. ∎

6. שדות של פונקציות אלגבריות

תהי F/K הרחבת שדות. אז $K' = \{\alpha \in F|\ K$ אלגברי מעל $\alpha\}$ הוא שדה ביניים של F/K. הוא נקרא **שדה הקבועים** של F (מעל K).

הגדרה 6.1: הרחבת שדות F/K נקראת **שדה פונקציות אלגבריות מעל** K אם F/K נוצרת סופית, שדה הקבועים שלה הוא K, ו־$F \neq K$.

אם $\mathrm{tr.\,deg}_K F = r$ אומרים כי F **שדה פונקציות אלגבריות ב־**r **משתנים מעל** K.

הערה 6.2: מעלת הטרנסצנדנטיות. קבוצה $T \subseteq F$ נקראת **בלתי תלויה אלגברית מעל** K אם לכל $t_1, \dots, t_n \in T$ שונים זה מזה ולכל $0 \neq f \in K[X_1, \dots, X_n]$ מתקיים $f(t_1, \dots, t_n) \neq 0$.

שני התנאים הבאים שקולים:

(א) T בלתי תלויה אלגברית מרבית ב־F מעל K.

(ב) T בלתי תלויה אלגברית מעל K ו־$F/K(T)$ אלגברית.

אם T מקיימת אותם, היא נקראת **בסיס טרנסצנדנטיות של** F **מעל** K.

כל שני בסיסי טרנסצנדנטיות של F/K הם שווי עוצמה. עוצמה זו מסומנת $\mathrm{tr.\,deg}_K F$ ונקראת **מעלת הטרנסצנדנטיות** של F/K. ∎

תרגיל 6.3: *הראה ששדה הפונקציות הרציונליות מעל K הוא שדה פונקציות אלגבריות במשתנה אחד.*

הערה 6.4: יהי F/K שדה פונקציות אלגבריות במשתנה אחד. לפי ההנחה $K \subsetneqq F$. יהי $x \in F \smallsetminus K$. אז x טרנסצנדנטי מעל K ובגלל ש־$\mathrm{tr.\,deg}_K F = 1$, הוא בסיס טרנסצנדיות של F/K ולכן $F/K(t)$ אלגברית. היא נוצרת סופית (כי F/K נוצרת סופית), לכן $[F : K(x)] < \infty$.

להיפך, אם F/K הרחבת שדות בעלת שדה קבועים $F \neq K$ ויש $x \in F$ כך ש־$[F : K(x)] < \infty$, אז F/K שדה פונקציות אלגבריות במשתנה אחד. ∎

טענה 6.5: *יהי F/K שדה פונקציות אלגבריות במשתנה אחד. יהי $\varphi\colon F \to L \cup \{\infty\}]$ אתר לא טריביאלי, טריביאלי על K. יהי $\bar{F}$ שדה השאריות של F. נזהה את $\varphi(K)$ עם K על ידי φ. אז*

(א) $K \subseteq \bar{F}$ ו־$[\bar{F} : K] < \infty$. *מספר זה ייקרא* **המעלה** $\deg \varphi$ *של* φ.

(ב) *לאתרים שקולים המעלות שוות.*

הוכחה: (א) כיוון ש־φ אינו טריביאלי, יש $t \in F$ כך ש־$\varphi(t) = \infty$. אז $t \notin K$. יהי $E = K(t)$. לפי הערה 6.4, $[F : E] < \infty$ ו־t טרנסצנדנטי מעל K. לפי הדיון בפרק 2, $\varphi|_E$ הוא אתר ששדה השאריות שלו הוא $\bar{E} = K$. לפי מסקנה 4.3, $[\bar{F} : \bar{E}] \le [F : E] < \infty$.

(ב) יהי $\mathcal{O}$ חוג ההערכה המתאים ל־φ ויהי m האידאל המרבי שלו. אז φ מעתיק את $\mathcal{O}$ על $\bar{F}$ ו־m הוא הגרעין. לכן יש איזומורפיזם $\mathcal{O}/m \cong \bar{F}$. כיוון ש־$K \subseteq \mathcal{O}$ ו־$K \cap m = 0$, איזומורפיזם זה מעתיק את התמונה

$m+K/m$ של K בתוך $\mathcal{O}/m$ על $\varphi(K)$. לכן $[\mathcal{O}/m : m+K/m] = [\bar{F} : K]$. כיוון שלאתר שקול אותו חוג ההערכה, גם המעלה שלו תהיה זהה לאגף ימין. ∎

יהי F/K שדה פונקציות אלגבריות. **הערכה של** F/K היא הערכה לא טריביאלית של F שהינה טריביאלית על K.

נחזור כאן על מסקנה 4.5 ומסקנה 3.3:

מסקנה 6.6: *יהי F/K שדה פונקציות אלגבריות במשתנה אחד. אז*

(א) *כל הערכה של F/K היא בדידה (ובפרט ארכימדית).*

(ב) *יהי $x \in F \smallsetminus K$. אז יש הערכות v, v' של F/K כך ש־$v'(x) < 0$ ו־$v(x) > 0$.*

תרגיל 6.7: *תהי F/K הרחבת שדות כך ש־K סגור אלגברית ב־F. הראה שאם $f \in K[X]$ אי פריק מעל K אז הוא אי פריק מעל F.*

הוכחה: בלי הגבלת הכלליות f מתוקן. יהי $\tilde{F}$ סגור אלגברי של F ויהי $\tilde{K} \subseteq \tilde{F}$ סגור אלגברי של K. די להראות כי אם $g \in F[X]$ גורם אי פריק מתוקן של f מעל F אז $g = f$.

יהי $g = (X-\alpha_1)\cdots(X-\alpha_m)$ הפירוק של g מעל $\tilde{F}$. אז $\alpha_1, \ldots, \alpha_m$ הם (חלק מן) שרשי f. בפרט $\alpha_1, \ldots, \alpha_m \in \tilde{K}$. מקדמי g הם פולינומים סימטריים יסודיים ב־$\alpha_1, \ldots, \alpha_m$, לכן הם ב־$\tilde{K}$. מכאן שהם ב־$\tilde{K} \cap F = K$, כלומר, $g \in K[X]$. לכן $g = f$. ∎

7. מחלקים

יהי F שדה פונקציות אלגבריות במשתנה אחד מעל K.

הגדרה 7.1: (א) **מחלק ראשוני** (prime divisor) **של** F/K הוא מחלקת שקילות של אתרים על F שהינם טריביאליים על K.

תהי $\mathbb{P}$ קבוצת כל המחלקים הראשוניים של F/K. לכל $\mathfrak{p} \in \mathbb{P}$ תהי $v_\mathfrak{p}$ הערכה מתאימה, $v_\mathfrak{p}(F^\times) = \mathbb{Z}$.

(ב) תהי $\tilde{\mathcal{D}}$ קבוצת כל הביטויים הפורמליים מהצורה $\sum_{\mathfrak{p}\in\mathbb{P}} n_\mathfrak{p}\mathfrak{p}$ באשר $n_\mathfrak{p} \in \mathbb{Z}$ לכל $\mathfrak{p} \in \mathbb{P}$. (במלים אחרות, $\tilde{\mathcal{D}}$ היא קבוצת הפונקציות מ־$\mathbb{P}$ לתוך $\mathbb{Z}$.) אז $\tilde{\mathcal{D}}$ חבורה ביחס לחיבור לפי הרכיבים.

(ג) לכל $\mathfrak{q} \in \mathbb{P}$ נגדיר $v_\mathfrak{q} \colon \tilde{\mathcal{D}} \to \mathbb{Z}$ על ידי $v_\mathfrak{q}(\sum_{\mathfrak{p}\in\mathbb{P}} n_\mathfrak{p}\mathfrak{p}) = n_\mathfrak{q}$. אזי $v_\mathfrak{q}$ הומומורפיזם של חבורות.

(ד) לכל $x \in F^\times$ נגדיר $(x) = \sum_{\mathfrak{p}\in\mathbb{P}} v_\mathfrak{p}(x)\mathfrak{p} \in \tilde{\mathcal{D}}$. אז $x \in K$ אם ורק אם $(x) = 0$.

(ה) נגדיר יחס סדר חלקי על $\tilde{\mathcal{D}}$ על ידי $\mathfrak{a} \le \mathfrak{b} \Leftrightarrow (\forall \mathfrak{p})\ v_\mathfrak{p}(\mathfrak{a}) \le v_\mathfrak{p}(\mathfrak{b})$. בפרט,

$$\max(\mathfrak{a},\mathfrak{b}) = \sum_{\mathfrak{p}\in\mathbb{P}} \max\big(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\big)\mathfrak{p} \in \tilde{\mathcal{D}}\,,$$
$$\min(\mathfrak{a},\mathfrak{b}) = \sum_{\mathfrak{p}\in\mathbb{P}} \min\big(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\big)\mathfrak{p} \in \tilde{\mathcal{D}}\,.$$

אם $\mathfrak{a} \le \mathfrak{b}$ ו־$\mathfrak{c} \in \tilde{\mathcal{D}}$ אז $\mathfrak{a}+\mathfrak{c} \le \mathfrak{b}+\mathfrak{c}$.

(ו) $\mathfrak{a} \in \tilde{\mathcal{D}}$ נקרא **מחלק של** F/K אם $v_\mathfrak{p}(\mathfrak{a}) = 0$ כמעט לכל $\mathfrak{p} \in \mathbb{P}$ (כלומר, פרט למספר סופי). תהי $\mathcal{D}$ קבוצת כל המחלקים של F/K. אז $\mathcal{D}$ תת חבורה של $\tilde{\mathcal{D}}$.

לכל $\mathfrak{a} \in \mathcal{D}$ מתקיים $\mathfrak{a} = \sum_\mathfrak{p} v_\mathfrak{p}(\mathfrak{a})\mathfrak{p}$.

(ז) **המעלה** $\deg\mathfrak{p}$ של מחלק ראשוני $\mathfrak{p}$ היא המעלה של אתר שמייצג את $\mathfrak{p}$. תמיד $\deg\mathfrak{p} \ge 1$.

(ח) **המעלה** $\deg\mathfrak{a}$ של מחלק $\mathfrak{a}$ מוגדרת על ידי $\deg\mathfrak{a} = \sum_\mathfrak{p} v_\mathfrak{p}(\mathfrak{a})\deg\mathfrak{p}$. זהו מספר שלם. ההעתקה $\deg \colon \mathcal{D} \to \mathbb{Z}$ היא הומומורפיזם של חבורות, שומר סדר חלקי.

(ט) תהי $S \subseteq \mathbb{P}$. לכל $\mathfrak{a} \in \tilde{\mathcal{D}}$ נגדיר $\mathfrak{a}_S \in \tilde{\mathcal{D}}$ על ידי $v_\mathfrak{p}(\mathfrak{a}_S) = \begin{cases} v_\mathfrak{p}(\mathfrak{a}) & \mathfrak{p} \in S \\ 0 & \mathfrak{p} \notin S \end{cases}$ וכן

$$\mathcal{L}(\mathfrak{a},S) = \{x \in F \mid v_\mathfrak{p}(x) + v_\mathfrak{p}(\mathfrak{a}) \ge 0 \text{ לכל } \mathfrak{p} \in S\} = \{x \in F \mid (x)_S + \mathfrak{a}_S \ge 0\}\,,$$
$$\mathcal{L}(\mathfrak{a}) = \{x \in F \mid v_\mathfrak{p}(x) + v_\mathfrak{p}(\mathfrak{a}) \ge 0 \text{ לכל } \mathfrak{p} \in \mathbb{P}\} = \mathcal{L}(\mathfrak{a},\mathbb{P})\,.$$

טענה 7.2: *תהי* $S \subseteq \mathbb{P}$ *ויהי* $\mathfrak{a} \in \tilde{\mathcal{D}}$.

(א) $\mathcal{L}(\mathfrak{a},S)$ *הוא מרחב וקטורי מעל* K *(תת מרחב של* F*).*

(ב) $\mathcal{L}(\mathfrak{a},S) = \mathcal{L}(\mathfrak{a}_S,S)$.

(ג) *אם* $S_1 \subseteq S_2$ *אז* $\mathcal{L}(\mathfrak{a},S_2) \subseteq \mathcal{L}(\mathfrak{a},S_1)$. *בפרט,* $\mathcal{L}(\mathfrak{a}) \subseteq \mathcal{L}(\mathfrak{a},S)$.

(ד) *יהי* $u \in F^\times$. *אז* $u\mathcal{L}(\mathfrak{a}, S) = \mathcal{L}\big(\mathfrak{a} - (u), S\big)$. *(שים לב, ש־* $x \mapsto ux$ *היא העתקה* $F \to F$ *לינארית־*K*.)*

הוכחה: (ד) לכל $x \in F$

$$x \in u\mathcal{L}(\mathfrak{a}, S) \Leftrightarrow x/u \in \mathcal{L}(\mathfrak{a}, S) \Leftrightarrow \text{לכל } \mathfrak{p} \in S\ \ v_\mathfrak{p}(x/u) + v_\mathfrak{p}(\mathfrak{a}) \geq 0 \Leftrightarrow$$

$$\Leftrightarrow \text{לכל } \mathfrak{p} \in S\ \ v_\mathfrak{p}(x) + v_\mathfrak{p}(\mathfrak{a}) - v_\mathfrak{p}(u) \geq 0 \Leftrightarrow x \in \mathcal{L}\big(\mathfrak{a} - (u), S\big).$$ ∎

למה 7.3: *תהי* $S \subseteq \mathbb{P}$ *קבוצה סופית ויהיו* $\mathfrak{a}, \mathfrak{b} \in \tilde{\mathcal{D}}$ *כך ש־* $\mathfrak{a} \leq \mathfrak{b}$. *אז* $\mathcal{L}(\mathfrak{a}, S) \subseteq \mathcal{L}(\mathfrak{b}, S)$ *ו־*

$$\dim_K \mathcal{L}(\mathfrak{b}, S)/\mathcal{L}(\mathfrak{a}, S) = \deg \mathfrak{b}_S - \deg \mathfrak{a}_S\,.$$

הוכחה: ההכלה ברורה. לפי טענה 7.2(ב) אפשר להניח כי $\mathfrak{a} = \mathfrak{a}_S, \mathfrak{b} = \mathfrak{b}_S$ מחלקים.

אם $U \subseteq W \subseteq V$ מרחבים וקטוריים מעל K אז $0 \to W/U \to V/U \to V/W \to 0$ סדרה מדויקת, ולכן לפי משפט המימד $\dim_K V/U = \dim_K V/W + \dim_K W/U$. בפרט אם $\mathfrak{c}$ מחלק כך ש־$\mathfrak{c} = \mathfrak{c}_S$ ו־$\mathfrak{a} \leq \mathfrak{c} \leq \mathfrak{b}$, אז $\mathcal{L}(\mathfrak{a}, S) \subseteq \mathcal{L}(\mathfrak{c}, S) \subseteq \mathcal{L}(\mathfrak{b}, S)$ ודי להוכיח

$$\dim_K \mathcal{L}(\mathfrak{b}, S)/\mathcal{L}(\mathfrak{c}, S) = \deg \mathfrak{b} - \deg \mathfrak{c}\,,$$

$$\dim_K \mathcal{L}(\mathfrak{c}, S)/\mathcal{L}(\mathfrak{a}, S) = \deg \mathfrak{c} - \deg \mathfrak{a}$$

כלומר, די להוכיח את השוויון המבוקש עבור $\mathfrak{a} \leq \mathfrak{c}$ ועבור $\mathfrak{c} \leq \mathfrak{b}$, במקום עבור $\mathfrak{a} \leq \mathfrak{b}$. לכן בלי הגבלת הכלליות $\mathfrak{b} = \mathfrak{a} + \mathfrak{p}$, באשר $\mathfrak{p} \in S$. אז צריך להוכיח

$$\dim_K \mathcal{L}(\mathfrak{a} + \mathfrak{p}, S)/\mathcal{L}(\mathfrak{a}, S) = \deg \mathfrak{p}\,. \tag{1}$$

לפי משפט הקירוב החלש קיים $u \in F$ כך ש־$v_\mathfrak{q}(u) = v_\mathfrak{q}(\mathfrak{a} + \mathfrak{p})$ לכל $\mathfrak{q} \in S$, כלומר, $(u)_S = \mathfrak{a} + \mathfrak{p}$. לפי טענה 7.2(ד), ההכפלה ב־u מעתיקה את $\mathcal{L}(\mathfrak{a} + \mathfrak{p}, S)$ על

$$\mathcal{L}(\mathfrak{a} + \mathfrak{p} - (u), S) = \mathcal{L}(\mathfrak{a} + \mathfrak{p} - (u)_S, S) = \mathcal{L}(0, S)$$

ובאופן דומה את $\mathcal{L}(\mathfrak{a}, S)$ על $\mathcal{L}(-\mathfrak{p}, S)$. לכן די להוכיח

$$\dim_K \mathcal{L}(0, S)/\mathcal{L}(-\mathfrak{p}, S) = \deg \mathfrak{p}\,. \tag{2}$$

נשים לב ש־$\mathcal{L}(0, S) \subseteq \mathcal{L}(0, \{\mathfrak{p}\}) = \mathcal{O}_\mathfrak{p}$, כי $\mathfrak{p} \in S$. יהי $\bar{F} = \mathcal{O}_\mathfrak{p}/m_\mathfrak{p}$ שדה השאריות של $\mathfrak{p}$.

טענה: *צמצום העתקת המנה* $\varphi\colon \mathcal{O}_\mathfrak{p} \to \bar{F}$ *ל־*$\mathcal{L}(0, S)$ *הוא על* $\bar{F}$ *וגרעינו* $\mathcal{L}(-\mathfrak{p}, S)$. אכן, יהי $\bar{x} \in \bar{F}$. אז יש $x \in \mathcal{O}_\mathfrak{p}$ כך ש־$\varphi(x) = \bar{x}$. לפי משפט הקירוב החלש קיים $y \in F$ כך ש־$v_\mathfrak{p}(y - x) > 0$ ו־$v_\mathfrak{q}(y) \geq 0$ לכל $\mathfrak{p} \neq \mathfrak{q} \in S$. מהאי שוויון הראשון נובע שגם $v_\mathfrak{p}(y) \geq 0$ ובפרט $y \in \mathcal{L}(0, S)$; בנוסף לכך, $\varphi(y - x) = 0$, לכן $\varphi(y) = \varphi(x) = \bar{x}$. לכן φ על.

כעת, יהי $x \in \mathcal{L}(0, S)$. אז $\varphi(x) = 0 \Leftrightarrow v_\mathfrak{p}(x) > 0 \Leftrightarrow v_\mathfrak{p}(x) \geq 1 \Leftrightarrow x \in \mathcal{L}(-\mathfrak{p}, S)$.

מהטענה נובע איזומורפיזם מרחבים וקטוריים מעל K, $\mathcal{L}(0, S)/\mathcal{L}(-\mathfrak{p}, S) \cong \bar{F}$. לכן ממדיהם שווים.

∎

תרגיל 7.4: *(א) יהי* $\mathfrak{a} \in \mathcal{D}$, $\mathfrak{a} < 0$. *אז* $\mathcal{L}(\mathfrak{a}) = 0$.

(ב) $\mathcal{L}(0) = K$.

הוכחה: (א) לכל מחלק $\mathfrak{p}$ מתקיים $v_{\mathfrak{p}}(\mathfrak{a}) \leq 0$ ויש $\mathfrak{q} \in \mathbb{P}$ עבורו $v_{\mathfrak{q}}(\mathfrak{a}) < 0$.

נניח שיש $0 \neq x \in \mathcal{L}(\mathfrak{a})$. אז $v_{\mathfrak{p}}(x) \geq -v_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ לכל $\mathfrak{p}$, ולכן לפי מסקנה 6.6(ב), $x \in K$, ו־$v_{\mathfrak{q}}(x) \geq -v_{\mathfrak{q}}(\mathfrak{a}) > 0$, סתירה.

(ב) אם $x \in K$ אז $v_{\mathfrak{p}}(x) = 0 \geq 0$ לכל $\mathfrak{p}$, לכן $x \in \mathcal{L}(0)$.

להיפך, אם $x \in \mathcal{L}(0)$, אז $v_{\mathfrak{p}}(x) \geq 0$ לכל $\mathfrak{p}$. לפי מסקנה 6.6(ב), $x \in K$. ∎

אם $\mathfrak{a} \in \mathcal{D}$ מחלק, אז $\mathcal{L}(\mathfrak{a})$ מרחב וקטורי מעל K. נסמן $\dim \mathfrak{a} = \dim_K \mathcal{L}(\mathfrak{a})$.

למה 7.5: *(א)* $\dim \mathfrak{a} < \infty$ *לכל* $\mathfrak{a} \in \mathcal{D}$.

(ב) *אם* $\mathfrak{b} \leq \mathfrak{a}$ *מחלקים, אז* $\dim \mathfrak{b} - \dim \mathfrak{a} \leq \deg \mathfrak{b} - \deg \mathfrak{a}$.

הוכחה: תהי S קבוצה כל המחלקים הראשוניים $\mathfrak{p}$ שמופיעים ב־$\mathfrak{a}$ או ב־$\mathfrak{b}$. אז S סופית ו־$\mathfrak{b} = \mathfrak{b}_S, \mathfrak{a} = \mathfrak{a}_S$.

טענה: $\mathcal{L}(\mathfrak{b}) \cap \mathcal{L}(\mathfrak{a}, S) = \mathcal{L}(\mathfrak{a})$.

אכן, ההכלות $\mathcal{L}(\mathfrak{a}) \subseteq \mathcal{L}(\mathfrak{a}, S)$ ו־$\mathcal{L}(\mathfrak{a}) \subseteq \mathcal{L}(\mathfrak{b})$ ברורות. להיפך, יהי $x \in \mathcal{L}(\mathfrak{b}) \cap \mathcal{L}(\mathfrak{a}, S)$, כלומר,

$$v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(\mathfrak{a}) \geq 0 \quad \text{לכל } \mathfrak{p} \in S, \qquad v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(\mathfrak{b}) \geq 0 \quad \text{לכל } \mathfrak{p} \in \mathbb{P}.$$

לפי הבחירה של S, $v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{b}) = 0$ לכל $\mathfrak{p} \in \mathbb{P} \smallsetminus S$. לכן $v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ לכל $\mathfrak{p} \in \mathbb{P} \smallsetminus S$. מכאן $v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ לכל $\mathfrak{p} \in \mathbb{P}$, כלומר, $x \in \mathcal{L}(\mathfrak{a})$. בכך הוכחה הטענה.

$$\begin{tikzcd}[arrows=-]
& \mathcal{L}(\mathfrak{b}, S) \arrow[d] & \\
& \mathcal{L}(\mathfrak{b}) + \mathcal{L}(\mathfrak{a}, S) \arrow[dl] \arrow[dr] & \\
\mathcal{L}(\mathfrak{b}) \arrow[dr] & & \mathcal{L}(\mathfrak{a}, S) \arrow[dl] \\
& \mathcal{L}(\mathfrak{a}) &
\end{tikzcd}$$

לפי משפט האיזומורפיזם השני $\mathcal{L}(\mathfrak{b})/\mathcal{L}(\mathfrak{a}) \cong \big(\mathcal{L}(\mathfrak{b}) + \mathcal{L}(\mathfrak{a}, S)\big)/\mathcal{L}(\mathfrak{a}, S) \leq \mathcal{L}(\mathfrak{b}, S)/\mathcal{L}(\mathfrak{a}, S)$, לכן לפי למה 7.3 ולפי בחירת S

$$\dim \mathcal{L}(\mathfrak{b})/\mathcal{L}(\mathfrak{a}) \leq \dim \mathcal{L}(\mathfrak{b}, S)/\mathcal{L}(\mathfrak{a}, S) = \deg \mathfrak{b}_S - \deg \mathfrak{a}_S = \deg \mathfrak{b} - \deg \mathfrak{a} \qquad (3)$$

הוכחה של (א): נבחר מחלק $\mathfrak{a}'$ כך ש־$\mathfrak{a}' < 0, \mathfrak{b}$. לפי תרגיל 7.4, $\mathcal{L}(\mathfrak{a}') = 0$. לפי (3),
$\dim \mathfrak{b} = \dim \mathcal{L}(\mathfrak{b})/0 \leq \deg \mathfrak{b} - \deg \mathfrak{a}' < \infty$.

הוכחה של (ב): אגף שמאל של (3) הוא $\dim \mathfrak{b} - \dim \mathfrak{a}$. ∎

מסקנה 7.6: *הפונקציה* $\deg \mathfrak{a} - \dim \mathfrak{a}$ *על המחלקים היא פונקציה עולה, כלומר, אם* $\mathfrak{a} \leq \mathfrak{b}$ *אז*
$\deg \mathfrak{a} - \dim \mathfrak{a} \leq \deg \mathfrak{b} - \dim \mathfrak{b}$.

בהמשך יתברר שלפונקציה זו יש חסם עליון.

מסקנה 7.7: *אם* $\mathfrak{b} \geq 0$ *מחלק אז* $\dim \mathfrak{b} \leq \deg \mathfrak{b} + 1$.

הוכחה: הצב $\mathfrak{a} = 0$ במסקנה הקודמת. כמובן, $\deg 0 = 0$; לפי תרגיל 7.4, $\dim \mathfrak{a} = 1$. לכן
$0 - 1 \leq \deg \mathfrak{b} - \dim \mathfrak{b}$. מכאן המסקנה. ∎

מסקנה 7.8: *אם* $\mathfrak{a}$ *מחלק ו־* $u \in F^\times$ *אז* $\dim \mathfrak{a} + (u) = \dim \mathfrak{a}$.

הוכחה: לפי טענה 7.2(ד), עם $S = \mathbb{P}$. ∎

תרגיל 7.9: *יהי* F/K *שדה פונקציות ויהי* $\mathfrak{a} \geq 0$ *מחלק שלו. אז לכל* $k \in \mathbb{N}$

$$\mathcal{L}\big((k-1)\mathfrak{a}\big) \subseteq \mathcal{L}\big(k\mathfrak{a}\big), \qquad \text{ו־} \dim\big((k-1)\mathfrak{a}\big) \leq \dim\big(k\mathfrak{a}\big) \leq \dim\big((k-1)\mathfrak{a}\big) + \deg \mathfrak{a}\,.$$

הוכחה: ההכלה ברורה, וממנה נובע האי שוויון השמאלי. כדי לקבל את הימני, נפעיל על ההכלה מסקנה 7.6:

$$\deg(k-1)\mathfrak{a} - \dim(k-1)\mathfrak{a} \leq \deg k\mathfrak{a} - \dim k\mathfrak{a}\,.$$

ומכאן

$$\dim k\mathfrak{a} \leq \dim(k-1)\mathfrak{a} + \deg k\mathfrak{a} - \deg(k-1)\mathfrak{a} = \dim(k-1)\mathfrak{a} + k \deg \mathfrak{a} - (k-1)\deg \mathfrak{a}$$
$$= \dim(k-1)\mathfrak{a} + \deg \mathfrak{a}\,. \quad ∎$$

תרגיל 7.10: *יהי* F/K *שדה פונקציות אלגבריות במשתנה אחד ויהי* $\mathfrak{p}$ *מחלק ראשוני שלו יהי* $x \in F^\times$. *הוכיחו:*
(א) אם $k \geq 0$ *שלם, אז:* $x \in \mathcal{L}\big(k\mathfrak{p}\big)$ *אם ורק אם* $(x)_\infty \leq k\mathfrak{p}$.
(ב) אם $k \geq 1$ *שלם, אז:* $x \in \mathcal{L}\big(k\mathfrak{p}\big) \smallsetminus \mathcal{L}\big((k-1)\mathfrak{p}\big)$ *אם ורק אם* $(x)_\infty = k\mathfrak{p}$.

הוכחה: (א) $x \in \mathcal{L}(k\mathfrak{p}) \Leftrightarrow (x) \geq -k\mathfrak{p} \Leftrightarrow v_\mathfrak{p}(x) \geq -k, v_\mathfrak{q}(x) \geq 0$ לכל $\mathfrak{p} \neq \mathfrak{q} \Leftrightarrow (x)_\infty \leq k\mathfrak{p}$.
(ב) לפי (א), $x \in \mathcal{L}\big(k\mathfrak{p}\big) \smallsetminus \mathcal{L}\big((k-1)\mathfrak{p}\big) \Leftrightarrow$
$\Leftrightarrow -k \leq v_\mathfrak{p}(x), 0 \leq v_\mathfrak{q}(x)$ לכל $\mathfrak{p} \neq \mathfrak{q}$, אבל $v_\mathfrak{p}(x) \ngeq -(k-1) \Leftrightarrow$
$\Leftrightarrow v_\mathfrak{p}(x) = -k, v_\mathfrak{q}(x) \geq 0$ לכל $\mathfrak{p} \neq \mathfrak{q} \Leftrightarrow (x)_\infty = k\mathfrak{p}$. ∎

8. מחלקים ראשיים

יהי F שדה פונקציות אלגבריות במשתנה אחד מעל K. נרחיב הגדרה 7.1(ד):

הגדרה 8.1: לכל $x \in F^\times$ נגדיר

$$\begin{aligned} \tilde{\mathcal{D}} \ni & \sum_{\mathfrak{p}\in\mathbb{P}} v_\mathfrak{p}(x)\mathfrak{p} &= (x), & \quad \text{המחלק של } x, \\ \tilde{\mathcal{D}} \ni & \sum_{\mathfrak{p}\in\mathbb{P},\, v_\mathfrak{p}(x)>0} v_\mathfrak{p}(x)\mathfrak{p} &= (x)_0, & \quad \text{מחלק האפסים של } x, \\ \tilde{\mathcal{D}} \ni & \sum_{\mathfrak{p}\in\mathbb{P},\, v_\mathfrak{p}(x)<0} v_\mathfrak{p}(x)\mathfrak{p} &= -(x)_\infty, & \quad \text{מחלק הקטבים של } x. \end{aligned}$$

(המלה "מחלק" תוצדק בהמשך.) אז

$$(x)_0 \geq 0,\ (x)_\infty \geq 0,\ (x) = (x)_0 - (x)_\infty,\ (x)_\infty = (x^{-1})_0,\ (x^{-1}) = -(x),$$
$$(xy) = (x) + (y), \quad m \in \mathbb{N} \text{ לכל } (x^m)_0 = m(x)_0,\ (x^m)_\infty = m(x)_\infty$$

למה 8.2: *יהי* $x \in F^\times$ *ותהי* $S \subseteq \mathbb{P}$ *סופית כך ש־* $v_\mathfrak{p}(x) > 0$ *לכל* $\mathfrak{p} \in S$*. אז* $\deg\,(x)_S \leq [F : K(x)]$.

הוכחה: בלי הגבלת הכלליות $x \notin K$. לכן x טרנסצנדנטי מעל K.

נסמן $\mathfrak{b} = (x)_S = \sum_{\mathfrak{p}\in S} v_\mathfrak{p}(x)\mathfrak{p}$. אז $\mathfrak{b} = \mathfrak{b}_S \geq 0$.

לפי למה 7.3, $\dim_K \mathcal{L}(\mathfrak{b}, S)/\mathcal{L}(0, S) = \deg \mathfrak{b}_S - \deg 0_S = \deg \mathfrak{b}$. לכן די להוכיח

טענה א: *יהי* $k > [F : K(x)]$ *ויהיו* $y_1, \dots, y_k \in \mathcal{L}(\mathfrak{b}, S)$*. אז הם תלויים לינארית מעל* K *מודולו* $\mathcal{L}(0, S)$.

אכן, לפי בחירת k, $y_1, \dots, y_k \in F$ תלויים לינארית מעל $K(x)$. לכן יש $f_1(x), \dots, f_k(x) \in K(x)$ לא כולם אפס, כך ש־$\sum_i f_i(x)y_i = 0$. עלינו למצוא $a_1, \dots, a_k \in K$, לא כולם אפס, כך ש־$\sum_i a_i y_i \in \mathcal{L}(0, S)$.

בלי הגבלת הכלליות $f_i(x) \in K[x]$ לכל i (אחרת נכפיל את $f_1(x), \dots, f_k(x)$ במכנה משותף) ולא כולם מתחלקים ב־x בחוג $K[x]$ (אחרת נחלק אותם בחזקה מתאימה של x). אז, לכל i, $f_i(x) = g_i(x) + a_i$, באשר $a_i \in K$ ו־$g_i \in K[x]$ מתחלק ב־x, ולא כל a_i הוא אפס. מתקיים $\sum_i a_i y_i = -\sum_i g_i(x)y_i$. לכן די להוכיח

טענה ב: *יהי* $g(x) \in K[x]$ *שמתחלק ב־x ויהי* $y \in \mathcal{L}(\mathfrak{b}, S)$*. אז* $g(x)y \in \mathcal{L}(0, S)$.

תחילה נשים לב ש־ $(g(x))_S \geq \mathfrak{b}$. אכן, $g(x) = \sum_{j\geq 1} c_j x^j$, לכן

$v_\mathfrak{p}(g(x)) \geq \min_{j\geq 1}\big(v_\mathfrak{p}(c_j) + jv_\mathfrak{p}(x)\big) \geq v_\mathfrak{p}(x)$ לכל $\mathfrak{p} \in S$, כלומר, $(g(x))_S \geq \mathfrak{b}$.

אם $g(x) = 0$, טענה ב ברורה. אם $g(x) \neq 0$ אז לפי טענה 7.2(ד),

$g(x)y \in g(x)\mathcal{L}(\mathfrak{b}, S) = \mathcal{L}(\mathfrak{b} - (g(x)), S) = \mathcal{L}(\mathfrak{b} - (g(x))_S, S) \subseteq \mathcal{L}(\mathfrak{b} - \mathfrak{b}, S) = \mathcal{L}(0, S)$. ∎

מסקנה 8.3: *יהי* $x \in F^\times$. *אז*

(א) $(x), (x)_0, (x)_\infty$ *הם מחלקים (נקראים* **מחלק הקטבים, מחלק האפסים והמחלק של** x*).*

(ב) $(x) = 0$ *אם ורק אם* $x \in K$.

(ג) *יהי* $x \in F \smallsetminus K$. *אז* $\deg(x)_0, \deg(x)_\infty \leq [F : K(x)]$.

הוכחה: אם $x \in K$, אז $(x) = 0$ וטענות (א), (ג) ברורות. יהי $x \in F \smallsetminus K$. אז $(x) \neq 0$ לפי מסקנה 6.6(ב). לפי הלמה הקודמת, $(x)_0$ מחלק ו־$\deg(x)_0 \leq [F : K(x)]$. נציב x^{-1} במקום x, אז $(x)_\infty = (x^{-1})_0$ מחלק ו־$\deg(x)_\infty \leq [F : K(x)]$. לכן גם $(x) = (x)_0 - (x)_\infty$ מחלק. ∎

הגדרה 8.4: **(א)** מחלק מהצורה $(x) = \sum_{\mathfrak{p} \in \mathbb{P}} v_\mathfrak{p}(x)\mathfrak{p}$, באשר $x \in F^\times$, נקרא **מחלק ראשי.**

(ב) אוסף כל המחלקים הראשיים $\mathcal{P} = \{(x) |\ x \in F^\times\}$ הוא תת חבורה של $\mathcal{D}$.

(ג) חבורת המנה $\mathcal{C} := \mathcal{D}/\mathcal{P}$ נקראת **חבורת מחלקות המחלקים.** ∎

הערה 8.5: ההעתקה $x \mapsto (x)$ משרה אפימורפיזם $F^\times \to \mathcal{P}$ שגרעינו $K^\times$. לכן קיימת סדרה מדויקת $0 \to K^\times \to F^\times \to \mathcal{D} \to \mathcal{C} \to 1$. ∎

למה 8.6: *יהי* $x \in F \smallsetminus K$ *ויהיו* $y_1, \ldots, y_n \in F$.

(א) *אם* $y_1, \ldots, y_n \in F$ *בלתי תלויים לינארית מעל* $K(x)$ *אז* $\{x^i y_j\}_{i=0}^{\infty}{}_{j=1}^{n}$ *בלתי תלויים לינארית מעל* K.

(ב) *קיים* $0 \neq g \in K[x]$ *כך ש־* $gy_1, \ldots, gy_n \in F$ *שלמים מעל* $K[x]$.

הוכחה: (א) כיוון ש־x טרנסצנדנטי מעל K, $\{x^i\}_{i=0}^{\infty}$ בלתי תלויים לינארית מעל K. מכאן הטענה נובעת בקלות:

יהי $k \in \mathbb{N}$ ותהי $\{a_{ij}\}_{i=0}^{k}{}_{j=1}^{n} \subseteq K$ כך ש־$\sum_j \sum_i a_{ij} x^i y_j = 0$. אז $\sum_i a_{ij} x^i \in K(x)$ לכל j ו־$\sum_j \left(\sum_i a_{ij} x^i \right) y_j = 0$, לכן, כיוון ש־$y_1, \ldots, y_n$ בלתי תלויים לינארית מעל $K(x)$, מתקיים $\sum_i a_{ij} x^i = 0$ לכל j. כיוון ש־$\{x^i\}_{i=0}^{k}$ בלתי תלויים לינארית מעל K, מתקיים $a_{ij} = 0$ לכל i, לכל j. לכן $\{x^i y_j\}_{i=0}^{k}{}_{j=1}^{n}$ בלתי תלויים לינארית מעל K, לכל k. זה שקול לתנאי (א). מתקיים

(ב) תזכורת: אם $R \subseteq S$ הרחבת חוגים, אז $y \in S$ **שלם מעל** R אם קיים פולינום $h(X) \in R[X]$ *מתוקן* כך ש־$h(y) = 0$.

יהי $1 \leq j \leq n$. אז $y := y_j$ אלגברי מעל $K(x)$, לכן יש $d \geq 1$ ו־$f_0, \ldots, f_{d-1} \in K(x)$ כך ש־

$$y^d + f_{d-1} y^{d-1} + \cdots + f_1 y + f_0 = 0. \tag{1}$$

כל f_i הוא מנה של שני פולינומים ב־$K[x]$; אם $0 \neq g \in K[x]$ כפולה משותפת (כלשהי) של כל המכנים שלהם, אז $f_i = g_i/g$, באשר $g_i \in K[x]$ לכל i. נכפיל את (1) ב־g^d. אז

$$(gy)^d + (gf_{d-1})(gy)^{d-1} + \cdots + g^{d-1} f_1 (gy) + g^d f_0 = 0.$$

ומכאן ברור ש־gy שלם מעל $K[x]$.

ברור שאפשר לבחור את g כך שיתאים לכל y_j ומכאן המסקנה. ∎

למה 8.7: *יהי* $x \in F$ *ויהי* $y \in F$ *שלם מעל* $K[x]$. *יהי* $\mathfrak{p} \in \mathbb{P}$. *אם* $v_{\mathfrak{p}}(x) \geq 0$ *אז* $v_{\mathfrak{p}}(y) \geq 0$.

הוכחה: מתקיים

$$y^d + f_{d-1}(x)y^{d-1} + \cdots + f_1(x)y + f_0(x) = 0, \qquad (1)$$

באשר $f_i(x) \in K[x]$ לכל i. בלי הגבלת הכלליות $y \neq 0$. אז

$$y = -f_{d-1}(x) - f_{d-2}(x)y^{-1} - \cdots - f_0(x)(y^{-1})^{d-1}. \qquad (2)$$

לפי ההנחה $v_{\mathfrak{p}}(x) \geq 0$ מתקיים $v_{\mathfrak{p}}(f_i(x)) \geq 0$ לכל i. אילו היה $v_{\mathfrak{p}}(y) < 0$, היה $v_{\mathfrak{p}}(y^{-1}) > 0$, ולכן אגף ימין של (2) היה בעל הערכה אי שלילית, בסתירה ל־$v_{\mathfrak{p}}(y) < 0$. ∎

משפט 8.8: *יהי* $x \in F \smallsetminus K$. *אז* $\deg(x)_0 = \deg(x)_\infty = [F : K(x)]$ *ולכן* $\deg(x) = 0$.

הוכחה: הטענה האחרונה נובעת מתוך $(x) = (x)_0 - (x)_\infty$. די להוכיח כי $\deg(x)_\infty = [F : K(x)]$, כי $(x)_0 = (x^{-1})_\infty$ ו־$K(x) = K(x^{-1})$. לפי מסקנה 8.3 די להוכיח כי $\deg(x)_\infty \geq [F : K(x)]$.

יהי $n = [F : K(x)]$ ויהיו $y_1, \ldots, y_n \in F$ בלתי תלויים לינארית מעל $K(x)$. לפי למה 8.6(ב) אפשר להניח שהם שלמים מעל $K[x]$. לפי הלמה הקודמת מתקיים לכל $\mathfrak{p} \in \mathbb{P}$: אם יש $1 \leq j \leq n$ כך ש־$v_{\mathfrak{p}}(y_j) < 0$ אז $v_{\mathfrak{p}}(x) < 0$. כלומר, אם יש $1 \leq j \leq n$ כך ש־$v_{\mathfrak{p}}((y_j)_\infty) > 0$ אז $v_{\mathfrak{p}}((x)_\infty) > 0$. כיוון שלפי מסקנה 8.3 יש רק מספר סופי של $\mathfrak{p}$ שמקיימים $v_{\mathfrak{p}}((x)_\infty) > 0$, עבור $k \in \mathbb{N}$ גדול מספיק מתקיים

$$k(x)_\infty \geq (y_j)_\infty, \qquad j = 1, \ldots, n.$$

כעת יהי $\ell \geq 0$ שלם כלשהו. אז לכל $0 \leq i \leq \ell$

$$\begin{aligned}(x^i y_j) + (k+\ell)(x)_\infty &= i(x) + (y_j) + k(x)_\infty + \ell(x)_\infty = \\ &= i(x)_0 - i(x)_\infty + (y_j)_0 - (y_j)_\infty + k(x)_\infty + \ell(x)_\infty = \\ &= i(x)_0 + (y_j)_0 + \big(k(x)_\infty - (y_j)_\infty\big) + (\ell - i)(x)_\infty \geq 0\end{aligned}$$

לכן $\{x^i y_j\}_{i=0}^{\ell}{}_{j=1}^{n} \subseteq \mathcal{L}\big((k+\ell)(x)_\infty\big)$. לפי למה 8.6(א), $x^i y_j$ בלתי תלויים לינארית מעל K, לכן

$$\dim(k+\ell)(x)_\infty \geq n(\ell+1). \qquad (3)$$

כיוון ש־$(k+\ell)(x)_\infty \geq 0$, לפי מסקנה 7.7 $\deg(k+\ell)(x)_\infty + 1 \geq \dim(k+\ell)(x)_\infty$. לכן

$$(k+\ell)\deg(x)_\infty + 1 \geq n(\ell+1).$$

מכאן $\deg(x)_\infty \geq n\frac{(\ell+1)}{(k+\ell)} - \frac{1}{(k+\ell)} \underset{\ell\to\infty}{\longrightarrow} n$, לכן $\deg(x)_\infty \geq n$, ∎

מסקנה 8.9: *יהי* $x \in F \smallsetminus K$. *אז יש* $q \in \mathbb{Z}$ *כך ש־* $\deg m(x)_\infty - \dim m(x)_\infty \leq q$ *לכל* $m \in \mathbb{Z}$.

הוכחה: לפי (3), יש $k \in \mathbb{N}$ כך ש־ $\dim m(x)_\infty \geq (m-k+1)\deg(x)_\infty$ לכל $m \geq k$. לכן

$$\deg m(x)_\infty - \dim m(x)_\infty \leq (k-1)\deg(x)_\infty \qquad (4)$$

לכל $m \geq k$. לפי מסקנה 7.6, אי שוויון זה נכון גם עבור $m < k$. ∎

9. משפט רימן

יהי F שדה פונקציות אלגבריות במשתנה אחד מעל K.

משפט 9.1 (משפט רימן): *יהי* $x \in F \setminus K$. *יהי* $q = \max_m \deg m(x)_\infty - \dim m(x)_\infty$. *אז* $q \geq -1$ *ולכל מחלק* $\mathfrak{a}$ *מתקיים*

$$\deg \mathfrak{a} - \dim \mathfrak{a} \leq q .$$

הוכחה: ההגדרה של q טובה לפי מסקנה 8.9. הטענה $q \geq -1$ תנבע מתרגיל 7.4(ב), כי $\dim 0 = 1$, $\deg 0 = 0$.

בלי הגבלת הכלליות $\mathfrak{a} \geq 0$, אחרת נבחר $\mathfrak{b} \geq 0$ כך ש־$\mathfrak{a} \leq \mathfrak{b}$; כיוון שלפי מסקנה 7.6 (בה נשתמש שוב ושוב)

$$\deg \mathfrak{a} - \dim \mathfrak{a} \leq \deg \mathfrak{b} - \dim \mathfrak{b} ,$$

די להוכיח את טענה עבור $\mathfrak{a} \geq 0$.

כעת $m(x)_\infty - \mathfrak{a} \leq m(x)_\infty$, לכן

$$\deg \big(m(x)_\infty - \mathfrak{a}\big) - \dim \big(m(x)_\infty - \mathfrak{a}\big) \leq \deg \big(m(x)_\infty\big) - \dim \big(m(x)_\infty\big) \leq q$$

מכאן

$$\dim \big(m(x)_\infty - \mathfrak{a}\big) \geq \deg \big(m(x)_\infty - \mathfrak{a}\big) - q = m \deg (x)_\infty - \deg \mathfrak{a} - q > 0$$

עבור m גדול מספיק. לכן קיים $0 \neq z \in \mathcal{L}\big(m(x)_\infty - \mathfrak{a}\big)$. הוא מקיים $(z) + m(x)_\infty - \mathfrak{a} \geq 0$, כלומר $\mathfrak{a} + (z^{-1}) \leq m(x)_\infty$. לכן

$$\deg \big(\mathfrak{a} + (z^{-1})\big) - \dim \big(\mathfrak{a} + (z^{-1})\big) \leq \deg \big(m(x)_\infty\big) - \dim \big(m(x)_\infty\big) \leq q$$

אבל $\deg \big(\mathfrak{a} + (z^{-1})\big) = \deg \mathfrak{a} + \deg (z^{-1}) = \deg \mathfrak{a}$ ולפי מסקנה 7.8, $\dim \big(\mathfrak{a} + (z^{-1})\big) = \dim \mathfrak{a}$, לכן $\deg \mathfrak{a} - \dim \mathfrak{a} \leq q$. ∎

נסמן $g = q + 1$.

מסקנה 9.2: *קיים* $g \geq 0$ *שלם המקיים*

(א) $g - 1 = \max_{\mathfrak{a} \in \mathcal{D}} \big(\deg \mathfrak{a} - \dim \mathfrak{a}\big)$.

(ב) $g - 1 = \max_m \big(\deg m(x)_\infty - \dim m(x)_\infty\big)$ *לכל* $x \in F \setminus K$.

הוא שמורה של $\mathrm{F/K}$ *וייקרא* ***הגזע*** (genus) *של* F/K.

10. אדלים

יהי F שדה פונקציות אלגבריות במשתנה אחד מעל K.

שאלה 10.1: לכל $\mathfrak{p} \in \mathbb{P}$ יהי $a_\mathfrak{p} \in F$. האם קיים $x \in F$ כך ש־$v_\mathfrak{p}(x - a_\mathfrak{p}) \geq 0$ לכל $\mathfrak{p} \in \mathbb{P}$?

נניח שכן. אם $v_\mathfrak{p}(a_\mathfrak{p}) < 0$, אז גם $v_\mathfrak{p}(x) < 0$. לפי מסקנה 8.3(א), זה קורה לכל היותר עבור מספר סופי של $\mathfrak{p}$. לכן תנאי הכרחי לקיום x כנ"ל הוא: $v_\mathfrak{p}(a_\mathfrak{p}) \geq 0$ עבור כמעט כל $\mathfrak{p} \in \mathbb{P}$. ∎

מכאן ההגדרה הבאה:

הגדרה 10.2: (א) **אָדֵל** של F/K הוא פונקציה $\alpha\colon \mathbb{P} \to F$ כך ש־$v_\mathfrak{p}(\alpha_\mathfrak{p}) \geq 0$ עבור כמעט כל $\mathfrak{p} \in \mathbb{P}$ (כתיב: $\alpha_\mathfrak{p} := \alpha(\mathfrak{p})$).

(ב) קבוצת כל האדלים $\mathbb{A}$ של F/K היא אלגברה (קומוטטיבית) מעל F ביחס לפעולת הבאות:

$$(\alpha+\beta)_\mathfrak{p} = \alpha_\mathfrak{p} + \beta_\mathfrak{p}, \quad (\alpha\beta)_\mathfrak{p} = \alpha_\mathfrak{p}\beta_\mathfrak{p}, \quad (x\alpha)_\mathfrak{p} = x\alpha_\mathfrak{p}, \qquad x \in F,\ \alpha,\beta \in \mathbb{A}.$$

(ג) קיים שיכון $F \to \mathbb{A}$ על ידי $x \mapsto [x] := x \cdot 1$, לכן ניתן לזהות את F כתת שדה של $\mathbb{A}$. כלומר, כל $x \in F$ מזוהה עם האדל $[x]$ הנתון על ידי $[x]_\mathfrak{p} = x$ לכל $\mathfrak{p} \in \mathbb{P}$.

(ד) נרחיב את $v_\mathfrak{p}$ מ־F לפונקיציה על $\mathbb{A}$ על ידי $v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(\alpha_\mathfrak{p})$. אז

$$v_\mathfrak{p}(\alpha\beta) = v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\beta), \quad v_\mathfrak{p}(\alpha+\beta) \geq \min\big(v_\mathfrak{p}(\alpha), v_\mathfrak{p}(\beta)\big).$$

(ה) לכל מחלק $\mathfrak{a} \in \mathcal{D}$ נגדיר $\Lambda(\mathfrak{a}) = \{\alpha \in \mathbb{A} |\ v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\mathfrak{a}) \geq 0 \text{ לכל } \mathfrak{p} \in \mathbb{P}\}$. ∎

תרגיל 10.3: *יהיו $\mathfrak{a}, \mathfrak{b}$ מחלקים. אז*

(א) *$\Lambda(\mathfrak{a})$ הוא מרחב וקטורי מעל K, תת מרחב של $\mathbb{A}$ מעל K.*

(ב) $\mathcal{L}(\mathfrak{a}) = F \cap \Lambda(\mathfrak{a})$.

(ג) *אם $\mathfrak{a} \leq \mathfrak{b}$ אז* $\Lambda(\mathfrak{a}) \subseteq \Lambda(\mathfrak{b})$.

(ד) $\Lambda(\mathfrak{a}) \cap \Lambda(\mathfrak{b}) = \Lambda\big(\min(\mathfrak{a},\mathfrak{b})\big)$.

(ה) $\Lambda(\mathfrak{a}) + \Lambda(\mathfrak{b}) = \Lambda\big(\max(\mathfrak{a},\mathfrak{b})\big)$.

(ו) *יהי $x \in F$. אז* $x\Lambda(\mathfrak{a}) = \Lambda\big(\mathfrak{a} - (x)\big)$.

פתרון: (ה) יהי $\mathfrak{c} = \max(\mathfrak{a},\mathfrak{b})$. אז $\mathfrak{a},\mathfrak{b} \leq \mathfrak{c}$, לכן לפי (ג), $\Lambda(\mathfrak{a}), \Lambda(\mathfrak{b}) \subseteq \Lambda(\mathfrak{c})$ ומכאן $\Lambda(\mathfrak{a}) + \Lambda(\mathfrak{b}) \subseteq \Lambda(\mathfrak{c})$.

להיפך, יהי $\gamma \in \Lambda(\mathfrak{c})$. יהי $\mathfrak{p} \in \mathbb{P}$. נבדיל בין שני מקרים:

(1) אם $v_\mathfrak{p}(\mathfrak{b}) < v_\mathfrak{p}(\mathfrak{a})$, אז $-v_\mathfrak{p}(\mathfrak{b}) > -v_\mathfrak{p}(\mathfrak{a})$ ו־$v_p(\mathfrak{b}) = v_\mathfrak{p}(\mathfrak{c})$. במקרה זה נבחר $\alpha_\mathfrak{p} \in F$ כך ש־$v_\mathfrak{p}(\alpha_\mathfrak{p}) \geq -v_\mathfrak{p}(\mathfrak{a})$ ונגדיר $\beta_\mathfrak{p} = \gamma_\mathfrak{p} - \alpha_\mathfrak{p}$. אז גם $v_\mathfrak{p}(\alpha_\mathfrak{p}) \geq -v_\mathfrak{p}(\mathfrak{b})$ ומתקיים $v_\mathfrak{p}(\gamma_\mathfrak{p}) \geq -v_\mathfrak{p}(\mathfrak{c}) = -v_\mathfrak{p}(\mathfrak{b})$. לכן $v_\mathfrak{p}(\beta_\mathfrak{p}) \geq \min(v_\mathfrak{p}(\alpha_\mathfrak{a}), v_\mathfrak{p}(\gamma_\mathfrak{p})) \geq -v_\mathfrak{p}(\mathfrak{b})$.

(2) אם $v_\mathfrak{p}(\mathfrak{a}) \ge v_\mathfrak{p}(\mathfrak{b})$, אז $-v_\mathfrak{p}(\mathfrak{b}) \ge -v_\mathfrak{p}(\mathfrak{a})$ ו־$v_\mathfrak{p}(\mathfrak{c}) = v_p(\mathfrak{a})$. במקרה זה נבחר $\beta_\mathfrak{p} \in F$ כך ש־$v_\mathfrak{p}(\beta_\mathfrak{p}) \ge -v_\mathfrak{p}(\mathfrak{b})$ ונגדיר $\alpha_\mathfrak{p} = \gamma_\mathfrak{p} - \beta_\mathfrak{p}$. אז גם $v_\mathfrak{p}(\beta_\mathfrak{p}) \ge -v_\mathfrak{p}(\mathfrak{a})$ ומתקיים $v_\mathfrak{p}(\gamma_\mathfrak{p}) \ge -v_\mathfrak{p}(\mathfrak{c}) = -v_\mathfrak{p}(\mathfrak{a})$. לכן $v_\mathfrak{p}(\alpha_\mathfrak{p}) \ge \min(v_\mathfrak{p}(\beta_\mathfrak{a}), v_\mathfrak{p}(\gamma_\mathfrak{p})) \ge -v_\mathfrak{p}(\mathfrak{a})$.

כמעט לכל $\mathfrak{p} \in \mathbb{P}$ מתקיים $v_\mathfrak{p}(\mathfrak{a}) = v_\mathfrak{p}(\mathfrak{b}) = 0$, ואז, לפי מקרה (2), מתקיים $v_\mathfrak{p}(\alpha_\mathfrak{p}), v_\mathfrak{p}(\beta_\mathfrak{p}) \ge 0$. לכן $(\alpha_\mathfrak{p}), (\beta_\mathfrak{p})$ מגדירים אדלים $\alpha, \beta \in \mathbb{A}$ שמקיימים $\gamma = \alpha + \beta$ ו־$\alpha \in \Lambda(\mathfrak{a})$ ו־$\beta \in \Lambda(\mathfrak{b})$. לכן $\Lambda(\mathfrak{a}) + \Lambda(\mathfrak{b}) = \Lambda(\mathfrak{c})$. ∎

למה 10.4: *יהיו* $\mathfrak{b} \le \mathfrak{a}$ *מחלקים. אז* $\dim_K \Lambda(\mathfrak{b})/\Lambda(\mathfrak{a}) = \deg \mathfrak{b} - \deg \mathfrak{a}$.

הוכחה: תהי S קבוצת כל המחלקים הראשוניים שמופיעים ב־$\mathfrak{a}$ או ב־$\mathfrak{b}$. לפי למה 7.3,

$$\dim_K \mathcal{L}(\mathfrak{b}, S)/\mathcal{L}(\mathfrak{a}, S) = \deg \mathfrak{b} - \deg \mathfrak{a} \,.$$

לכן די להוכיח שקיים איזומורפיזם של מרחבים וקטוריים $\mathcal{L}(\mathfrak{b}, S)/\mathcal{L}(\mathfrak{a}, S) \to \Lambda(\mathfrak{b})/\Lambda(\mathfrak{a})$.

נגדיר $T\colon F \to \mathbb{A}$ על ידי $\big(T(x)\big)_\mathfrak{p} = \begin{cases} x & \mathfrak{p} \in S \\ 0 & \mathfrak{p} \notin S \end{cases}$. אז T העתקה לינארית מעל K. מתקיים $T\big(\mathcal{L}(\mathfrak{b}, S)\big) \subseteq \Lambda(\mathfrak{b})$, לכן T משרה העתקה לינארית $\bar{T}\colon \mathcal{L}(\mathfrak{b}, S) \to \Lambda(\mathfrak{b})/\Lambda(\mathfrak{a})$.

$$\begin{tikzcd}
\mathcal{L}(\mathfrak{b}, S) \arrow[r, "T"] \arrow[d] \arrow[dr, "\bar{T}"'] & \Lambda(\mathfrak{b}) \arrow[d] \\
\mathcal{L}(\mathfrak{b}, S)/\mathcal{L}(\mathfrak{a}, S) \arrow[r] & \Lambda(\mathfrak{b})/\Lambda(\mathfrak{a})
\end{tikzcd}$$

היא על. אכן, יהי $\beta \in \Lambda(\mathfrak{b})$. לפי משפט הקירוב החלש יש $b \in F$ כך ש־ $v_\mathfrak{p}(b - \beta_\mathfrak{p}) \ge -v_\mathfrak{p}(\mathfrak{a})$ לכל $\mathfrak{p} \in S$. אז $v_\mathfrak{p}(T(b) - \beta) \ge -v_\mathfrak{p}(\mathfrak{a})$ לכל $\mathfrak{p} \in S$. זה נכון גם עבור $\mathfrak{p} \notin S$, כי אז

$$v_\mathfrak{p}(T(b) - \beta) = v_\mathfrak{p}(\beta) \ge -v_\mathfrak{p}(\mathfrak{b}) = 0 = -v_\mathfrak{p}(\mathfrak{a}).$$

לכן $T(b) - \beta \in \Lambda(\mathfrak{a})$, כלומר, $T(b) \equiv \beta \mod \Lambda(\mathfrak{a})$.

לבסוף,

$$\begin{aligned}\operatorname{Ker} \bar{T} &= \{b \in \mathcal{L}(\mathfrak{b}, S) |\ T(b) \in \Lambda(\mathfrak{a})\} = \{b \in F |\ (\forall \mathfrak{p} \in \mathbb{P})\, v_\mathfrak{p}\big(T(b)\big) + v_\mathfrak{p}(\mathfrak{a}) \ge 0\} = \\ &= \{b \in F |\ (\forall \mathfrak{p} \in S)\, v_\mathfrak{p}(b) + v_\mathfrak{p}(\mathfrak{a}) \ge 0\} = \mathcal{L}(\mathfrak{a}, S)\end{aligned}$$

לכן $\bar{T}$ משרה לפי משפט האיזומורפיזם הראשון את האיזומורפיזם המבוקש. ∎

למה 10.5: *יהיו* $\mathfrak{b} \le \mathfrak{a}$ *מחלקים. אז*

$$(\deg \mathfrak{b} - \dim \mathfrak{b}) - (\deg \mathfrak{a} - \dim \mathfrak{a}) = \dim_K \big(\Lambda(\mathfrak{b}) + F\big)/\big(\Lambda(\mathfrak{a}) + F\big).$$

הוכחה: קיים התרשים הבא של הכלות של מרחבים וקטוריים מעל K

$$\begin{tikzcd}
& \Lambda(\mathfrak{b})+F \arrow[dl, dash] \arrow[dr, dash] & & \\
\Lambda(\mathfrak{a})+F \arrow[dr, dash] & & \Lambda(\mathfrak{b}) \arrow[dl, dash] \arrow[dr, dash] & \\
& \Lambda(\mathfrak{a}) \arrow[dr, dash] & & \mathcal{L}(\mathfrak{b}) \arrow[dl, dash] \\
& & \mathcal{L}(\mathfrak{a}) &
\end{tikzcd}$$

נוסיף אליו את $\Lambda(\mathfrak{a})+\mathcal{L}(\mathfrak{b})$:

$$\begin{tikzcd}
& \Lambda(\mathfrak{b})+F \arrow[dl, dash] \arrow[dr, dash] & \\
\Lambda(\mathfrak{a})+F \arrow[dr, dash] & & \Lambda(\mathfrak{b}) \arrow[dl, dash] \\
& \Lambda(\mathfrak{a})+\mathcal{L}(\mathfrak{b}) \arrow[dl, dash] \arrow[dr, dash] & \\
\Lambda(\mathfrak{a}) \arrow[dr, dash] & & \mathcal{L}(\mathfrak{b}) \arrow[dl, dash] \\
& \mathcal{L}(\mathfrak{a}) &
\end{tikzcd}$$

מתקיים (ראה תרגיל 10.3)

$$\big(\Lambda(\mathfrak{a})+F\big)+\Lambda(\mathfrak{b})=\big(\Lambda(\mathfrak{a})+\Lambda(\mathfrak{b})\big)+F=\Lambda(\mathfrak{b})+F$$

$$\big(\Lambda(\mathfrak{a})+F\big)\cap\Lambda(\mathfrak{b})=\Lambda(\mathfrak{a})+\big(F\cap\Lambda(\mathfrak{b})\big)=\Lambda(\mathfrak{a})+\mathcal{L}(\mathfrak{b})$$

$$\Lambda(\mathfrak{a})\cap\mathcal{L}(\mathfrak{b})=\Lambda(\mathfrak{a})\cap\Lambda(\mathfrak{b})\cap F=\Lambda(\mathfrak{a})\cap F=\mathcal{L}(\mathfrak{a})$$

לכן לפי משפטי האיזומורפיזם

$$\begin{aligned}
\big(\Lambda(\mathfrak{b})+F\big)/\big(\Lambda(\mathfrak{a})+F\big) &\cong \Lambda(\mathfrak{b})/\big(\Lambda(\mathfrak{a})+\mathcal{L}(\mathfrak{b})\big)\\
&\cong \Lambda(\mathfrak{b})/\Lambda(\mathfrak{a})\Big/\big(\Lambda(\mathfrak{a})+\mathcal{L}(\mathfrak{b})\big)/\Lambda(\mathfrak{a})
\end{aligned}$$

$$\big(\Lambda(\mathfrak{a})+\mathcal{L}(\mathfrak{b})\big)/\Lambda(\mathfrak{a})\cong\mathcal{L}(\mathfrak{b})/\mathcal{L}(\mathfrak{a})$$

לכן, לפי למה 10.4,

$$\dim_K \big(\Lambda(\mathfrak{b})+F\big)/\big(\Lambda(\mathfrak{a})+F\big) = \dim_K \Lambda(\mathfrak{b})/\Lambda(\mathfrak{a}) - \dim_K \mathcal{L}(\mathfrak{b})/\mathcal{L}(\mathfrak{a}) =$$
$$= (\deg \mathfrak{b} - \deg \mathfrak{a}) - (\dim \mathfrak{b} - \dim \mathfrak{a}) = (\deg \mathfrak{b} - \dim \mathfrak{b}) - (\deg \mathfrak{a} - \dim \mathfrak{a}) \quad \blacksquare$$

מסקנה 10.6: *יהי* $\mathfrak{a}$ *מחלק שמקיים* $g-1 = \deg \mathfrak{a} - \dim \mathfrak{a}$*. אז* $\Lambda(\mathfrak{a}) + F = \mathbb{A}$.

הוכחה: לפי מסקנה 9.2, $g-1 = \max_{\mathfrak{b}\in\mathcal{D}} \big(\deg \mathfrak{b} - \dim \mathfrak{b}\big)$. לכן לפי מסקנה 7.6, אם $\mathfrak{b} \geq \mathfrak{a}$ אז גם $g-1 = \deg \mathfrak{b} - \dim \mathfrak{b}$. לפי הלמה הקודמת

$$\dim_K \big(\Lambda(\mathfrak{b})+F\big)/\big(\Lambda(\mathfrak{a})+F\big) = (\deg \mathfrak{b} - \dim \mathfrak{b}) - (\deg \mathfrak{a} - \dim \mathfrak{a}) = 0 \,.$$

לכן $\Lambda(\mathfrak{b}) + F = \Lambda(\mathfrak{a}) + F$.

יהי $\alpha \in \mathbb{A}$. יש מחלק $\mathfrak{b}$ כך ש־$\mathfrak{b} \geq \mathfrak{a}$ ו־$v_\mathfrak{p}(\mathfrak{b}) \geq -v_\mathfrak{p}(\alpha)$ לכל $\mathfrak{p}$. אז $\alpha \in \Lambda(\mathfrak{b})$, לכן $\alpha \in \Lambda(\mathfrak{a}) + F$.

$\blacksquare$

משפט 10.7: *יהי* $\mathfrak{a}$ *מחלק. אז* $\dim_K \mathbb{A}/\big(\Lambda(\mathfrak{a})+F\big) = g - 1 - (\deg \mathfrak{a} - \dim \mathfrak{a})$.

הוכחה: לפי מסקנה 9.2 קיים מחלק $\mathfrak{b}$ כך ש־$\deg \mathfrak{b} - \dim \mathfrak{b} = \max_{\mathfrak{c}\in\mathcal{D}} \big(\deg \mathfrak{c} - \dim \mathfrak{c}\big)$ $g-1 =$. בלי הגבלת הכלליות $\mathfrak{a} \geq \mathfrak{b}$, אחרת נחליף את $\mathfrak{b}$ ב־$\max(\mathfrak{a},\mathfrak{b})$ ונשתמש במסקנה 7.6. לפי מסקנה 10.6, $\Lambda(\mathfrak{b})+F = \mathbb{A}$. נציב זאת ו־$g-1 = \deg \mathfrak{b} - \dim \mathfrak{b}$ בלמה 10.5 ונקבל את התוצאה. $\blacksquare$

תרגיל 10.8 (משפט קירוב): *הראה כי* $\Lambda(\mathfrak{a}) + F = \mathbb{A}$ *מתקיים אם ורק אם לכל* $\alpha \in \mathbb{A}$ *יש* $x \in F$ *כך ש־*$v_\mathfrak{p}(x - \alpha_\mathfrak{p}) \geq -v_\mathfrak{p}(\mathfrak{a})$ *לכל* $\mathfrak{p}$ *ראשוני.*

11. דיפרנציאלים

תרגיל 11.1: *תהי F/K הרחבת שדות. יהי V מרחב וקטורי מעל F ויהי W מרחב וקטורי מעל K. אז $\mathrm{Hom}_K(V,W)$ (אוסף כל ההעתקות הלינאריות־ K מ־ V לתוך W) הוא מרחב וקטורי מעל F בעזרת החיבור הרגיל של העתקות ובעזרת הכפל*

$$(aT)(v) = T(av), \qquad a \in F, T \in \mathrm{Hom}_K(V,W), v \in V.$$

(נשים לב: אם $a \in K$ אז $(aT)(v) = aT(v)$.)

יהי F שדה פונקציות אלגבריות במשתנה אחד מעל K.

אז מרחב האדֵלים $\mathbb{A}$ הוא מרחב וקטורי מעל F. אם נראה אותו כמרחב וקטורי מעל K, אז המרחב הדואלי שלו $\mathrm{Hom}_K(\mathbb{A},K)$ מוגדר. מרחב זה הוא, לפי התרגיל, מרחב וקטורי מעל F.

הגדרה 11.2: (א) **דיפרנציאל** של F/K היא העתקה לינארית $\omega \in \mathrm{Hom}_K(\mathbb{A},K)$ (כלומר, פונקציונל) אשר מתאפסת על תת מרחב מהצורה $\Lambda(\mathfrak{a}) + F$ של $\mathbb{A}$, באשר $\mathfrak{a}$ מחלק. אוסף כל הדיפרנציאלים יסומן Ω.

(ב) עבור מחלק $\mathfrak{a}$ נסמן $\Omega(\mathfrak{a}) = \{\omega \in \mathrm{Hom}_K(\mathbb{A},K) |\ \omega\big(\Lambda(\mathfrak{a}) + F\big) = 0\}$. זהו תת מרחב של $\mathrm{Hom}_K(\mathbb{A},K)$ כמרחב וקטורי מעל K. אז $\Omega = \bigcup_{\mathfrak{a}} \Omega(\mathfrak{a})$. נסמן $\delta(\mathfrak{a}) = \dim_K \Omega(\mathfrak{a})$. ∎

הערה 11.3:

(א) העתקה $\omega \in \mathrm{Hom}(\mathbb{A},K)$ מתאפסת על $\Lambda(\mathfrak{a}) + F$ אם ורק אם היא מתאפסת על F ועל $\Lambda(\mathfrak{a})$.

(ב) את $\Omega(\mathfrak{a})$ אפשר לזהות עם מרחב הפונקציונליים הלינאריים על $\mathbb{A}/\big(\Lambda(\mathfrak{a}) + F\big)$. לכן לפי משפט 10.7

מסקנה 11.4: $\delta(\mathfrak{a}) = \dim_K \Omega(\mathfrak{a}) = \dim_K \mathbb{A}/(\Lambda(\mathfrak{a}) + F) = g - 1 - (\deg \mathfrak{a} - \dim \mathfrak{a})$.

תרגיל 11.5: *יהיו $\mathfrak{a}, \mathfrak{b}$ מחלקים ויהי $x \in F^\times$. הוכח:*

(א) *אם* $\mathfrak{a} \le \mathfrak{b}$ *אז* $\Omega(\mathfrak{a}) \supseteq \Omega(\mathfrak{b})$.

(ב) $\Omega\big(\max(\mathfrak{a},\mathfrak{b})\big) = \Omega(\mathfrak{a}) \cap \Omega(\mathfrak{b})$.

(ג) $x\Omega(\mathfrak{a}) = \Omega\big(\mathfrak{a} + (x)\big)$.

פתרון: לפי תרגיל 10.3.

(א) $\Lambda(\mathfrak{b}) \subseteq \Lambda(\mathfrak{a})$, לכן $\Omega(\mathfrak{a}) \supseteq \Omega(\mathfrak{b})$.

(ב) איבר בשני האגפים מתאפס על F. הוא באגף ימין אם ורק אם הוא מתאפס על $\Lambda(\mathfrak{a})$ וגם על $\Lambda(\mathfrak{b})$ אם ורק אם הוא מתאפס על $\Lambda(\mathfrak{a}) + \Lambda(\mathfrak{b})$, כלומר, על $\Lambda\big(\max(\mathfrak{a},\mathfrak{b})\big)$.

(ג) יהי ω פונקציונל על $\mathbb{A}$. לפי ההגדרה $(x\omega)(\alpha) = \omega(x\alpha)$. לכן אם ω מתאפס על F אז גם $x\omega$ מתאפס על F. כמו כן ω מתאפס על α אם ורק אם $x\omega$ מתאפס על $x^{-1}\alpha$. לכן $\omega \in \Omega(\mathfrak{a})$ אם ורק אם $x\omega$ מתאפס על $x^{-1}\Lambda(\mathfrak{a}) = \Lambda(\mathfrak{a} + (x))$, כלומר $x\omega \in \Omega(\mathfrak{a} + (x))$.

למה 11.6: *Ω הוא תת מרחב וקטורי של $\mathrm{Hom}_K(\mathbb{A}, K)$ מעל F.*

הוכחה: נראה ש־Ω סגור תחת החיבור ותחת הכפל בסקלרים של F. כזכור, $\Omega = \bigcup_{\mathfrak{c}} \Omega(\mathfrak{c})$.

יהיו $\omega_1, \omega_2 \in \Omega$. אז יש מחלק $\mathfrak{c}$ כך ש־ $\omega_1, \omega_2 \in \Omega(\mathfrak{c})$: אם $\omega_1 \in \Omega(\mathfrak{a}), \omega_2 \in \Omega(\mathfrak{b})$. אז, לפי תרגיל 11.5(א), $\omega_1, \omega_2 \in \Omega\big(\min(\mathfrak{a}, \mathfrak{b})\big)$. לכן $\omega_1 + \omega_2 \in \Omega(\mathfrak{c}) \subseteq \Omega$.

יהיו $x \in F^\times$, $\omega \in \Omega$. נניח $\omega \in \Omega(\mathfrak{a})$. לפי תרגיל 11.5(ג), $x\omega \in x\Omega(\mathfrak{a}) = \Omega\big(\mathfrak{a} + (x)\big) \subseteq \Omega$.

∎

משפט 11.7: *$\dim_F \Omega = 1$. כלומר, אם $\omega_1, \omega_2 \in \Omega$ שונים מאפס, אז יש $x \in F^\times$ יחיד כך ש־$\omega_2 = x\omega_1$.*

הוכחה: היחידות של x ברורה.

לפי תרגיל 11.5(א), יש $\mathfrak{b} \in \mathcal{D}$ כך ש־$\omega_1, \omega_2 \in \Omega(\mathfrak{b})$. נבחר $\mathfrak{a} \in \mathcal{D}$ שלילי כך ש־$\deg \mathfrak{a}$ קטן מאד. לפי תרגיל 7.4(א), $\dim \mathfrak{a} = 0$. לכן לפי מסקנה 11.4, $\dim \Omega(\mathfrak{a}) = g - 1 - \deg \mathfrak{a} > 0$.

יהי $1 \leq i \leq 2$. ההעתקה $x \mapsto x\omega_i$ היא העתקה חד חד ערכית $F \to \Omega$ לינארית מעל K (ואפילו מעל F). אם $x \in \mathcal{L}(\mathfrak{b} - \mathfrak{a})$ אז $(x) + \mathfrak{b} - \mathfrak{a} \geq 0$, כלומר, $(x) + \mathfrak{b} \geq \mathfrak{a}$, לכן לפי תרגיל 11.5(ג),(א), $x\omega_i \in x\Omega(\mathfrak{b}) = \Omega\big(\mathfrak{b} + (x)\big) \subseteq \Omega(\mathfrak{a})$. לכן $x \mapsto x\omega_i$ היא העתקה חד חד ערכית $T_i \colon \mathcal{L}(\mathfrak{b} - \mathfrak{a}) \to \Omega(\mathfrak{a})$ לינארית מעל K. לפי משפט רימן, $\deg(\mathfrak{b} - \mathfrak{a}) - \dim(\mathfrak{b} - \mathfrak{a}) \leq g - 1$. כיוון ש־$\deg \mathfrak{a}$ – גדול מאד,

$$\begin{aligned} \dim \mathrm{Im}\, T_i = \dim(\mathfrak{b} - \mathfrak{a}) &\geq \deg(\mathfrak{b} - \mathfrak{a}) + 1 - g = \\ &= \deg \mathfrak{b} - \deg \mathfrak{a} + 1 - g > \frac{1}{2}(g - 1 - \deg \mathfrak{a}) = \frac{1}{2} \dim \Omega(\mathfrak{a}) \end{aligned}.$$

(השוויון האחרון –לפי מסקנה 11.4.) לכן

$$\begin{aligned} \dim(\mathrm{Im}\, T_1 \cap \mathrm{Im}\, T_2) = \dim \mathrm{Im}\, T_1 + \dim \mathrm{Im}\, T_2 - \dim(\mathrm{Im}\, T_1 + \mathrm{Im}\, T_2) > \\ > 2 \cdot \frac{1}{2} \dim \Omega(\mathfrak{a}) - \dim \Omega(\mathfrak{a}) = 0 \end{aligned}$$

מכאן $\mathrm{Im}\, T_1 \cap \mathrm{Im}\, T_2 \neq 0$. לכן יש $x_1, x_2 \in F^\times$ כך ש־$x_1\omega_1 = x_2\omega_2$. יהי $x = \frac{x_1}{x_2}$. אז $x\omega_1 = \omega_2$.

∎

תרגיל 11.8: *הוכח ש־$g = \delta(0)$.*

פתרון: לפי תרגיל 7.4(ב), $\dim 0 = 1$; כמובן, $\deg 0 = 0$. לכן לפי מסקנה 11.4, $\delta(0) = g - 1 - (0 - 1) = g$

∎

משפט 11.9: *לכל $0 \neq \omega \in \Omega$ קיים מחלק יחיד $\mathfrak{b}$ כך ש־ω מתאפס על $\Lambda(\mathfrak{a})$ (כלומר, $\omega \in \Omega(\mathfrak{a})$) אם ורק אם $\mathfrak{a} \leq \mathfrak{b}$. מחלק זה יסומן (ω).*

הוכחה: יחידות: אם גם $\mathfrak{b}'$ מקיים את התנאי אז $\mathfrak{b}' \leq \mathfrak{b}$ וגם $\mathfrak{b} \leq \mathfrak{b}'$, לכן $\mathfrak{b} = \mathfrak{b}'$.

טענה: *יהי $\mathfrak{a}$ מחלק כך ש־$\omega \in \Omega(\mathfrak{a})$. אז $\dim \mathfrak{a} \le g$.* אכן, אם $\mathcal{L}(\mathfrak{a}) = 0$, אז $\dim \mathfrak{a} = 0 \le g$. אחרת יש $0 \ne x \in \mathcal{L}(\mathfrak{a})$. אז $\mathfrak{a} + (x) \ge 0$, לכן $x\omega \in x\Omega(\mathfrak{a}) = \Omega\big(\mathfrak{a} + (x)\big) \subseteq \Omega(0)$. לכן ההעתקה $x \mapsto x\omega$ היא מונומורפיזם $\mathcal{L}(\mathfrak{a}) \to \Omega(0)$ של מרחבים וקטוריים מעל K. מכאן, לפי תרגיל 11.8, $\dim \mathfrak{a} \le \delta(0) = g$.

בפרט לפי מסקנה 9.2,

$$\deg \mathfrak{a} \le g - 1 + \dim \mathfrak{a} \le 2g - 1 .$$

לכן קיים מחלק $\mathfrak{b}$ בעל מעלה מרבית כך ש־$\omega \in \Omega(\mathfrak{b})$.

אם $\omega \in \Omega(\mathfrak{a})$ אז $\omega \in \Omega(\mathfrak{a}) \cap \Omega(\mathfrak{b}) = \Omega\big(\max(\mathfrak{a}, \mathfrak{b})\big)$ ו־$\deg \max(\mathfrak{a}, \mathfrak{b}) \ge \deg \mathfrak{b}$, לכן , לפי בחירת $\mathfrak{b}$, מתקיים $\deg \max(\mathfrak{a}, \mathfrak{b}) = \deg \mathfrak{b}$. מכאן $\max(\mathfrak{a}, \mathfrak{b}) = \mathfrak{b}$. מכאן ש־$\mathfrak{a} \le \mathfrak{b}$. ∎

מסקנה 11.10: *יהי $0 \ne \omega \in \Omega$ ויהי $x \in F^\times$. אז $(x\omega) = (x) + (\omega)$.*

הוכחה: יהי $\mathfrak{a}$ מחלק. אז

$$x\omega \in \Omega(\mathfrak{a}) \Leftrightarrow \omega \in x^{-1}\Omega(\mathfrak{a}) = \Omega\big(\mathfrak{a} - (x)\big) \Leftrightarrow \mathfrak{a} - (x) \le (\omega) \Leftrightarrow \mathfrak{a} \le (\omega) + (x) \quad ∎$$

הגדרה 11.11: מחלק מהצורה (ω), באשר $0 \ne \omega \in \Omega$, ייקרא **קנוני**. נסמן ב־W את קבוצת המחלקים הקנוניים. ∎

מסקנה 11.12: *קבוצת W היא מחלקת מחלקים של F/K.*

הוכחה: יהי $0 \ne \omega_0 \in \Omega$. לפי משפט 11.7, $\Omega \smallsetminus \{0\} = \{x\omega_0 |\ x \in F^\times\}$. לכן לפי מסקנה 11.10

$$W = \{(x\omega_0) |\ x \in F^\times\} = \{(x) + (\omega_0) |\ x \in F^\times\}. \quad ∎$$

תרגיל 11.13: *הראה שהטענה הבאה איננה נכונה: יהיו $\mathfrak{a}, \mathfrak{b}$ מחלקים. אז $\Omega\big(\min(\mathfrak{a}, \mathfrak{b})\big) = \Omega(\mathfrak{a}) + \Omega(\mathfrak{b})$.*

פתרון: נמצא דוגמה נגדית.

יהי $0 \ne \omega \in \Omega$. יהי $\mathfrak{c} := (\omega)$ המחלק הקנוני המתאים לו. נבחר שני מחלקים ראשוניים שונים $\mathfrak{p}, \mathfrak{q}$ שאינם מופיעים ב־$\mathfrak{c}$ (כלומר, המקדם של הקואורדינטות ה־$\mathfrak{p}$ וה־$\mathfrak{q}$ בהצגה של $\mathfrak{c}$ הוא 0), ונגדיר $\mathfrak{a} = \mathfrak{c} + \mathfrak{p},\ \mathfrak{b} = \mathfrak{c} + \mathfrak{q}$. אז

$$(\omega) = \mathfrak{c} = \min(\mathfrak{a}, \mathfrak{b}).$$

לפי משפט 11.9, $\omega \in \Omega(\mathfrak{c})$.

טענה: *אין קיימים $\omega_1 \in \Omega(\mathfrak{a}),\ \omega_2 \in \Omega(\mathfrak{b})$ כך ש־$\omega = \omega_1 + \omega_2$.*

אכן, נניח בשלילה שהם קיימים. אז $\omega_1 \ne 0$, אחרת $\omega = \omega_2 \in \Omega(\mathfrak{b})$, ואז, לפי משפט 11.9, $\mathfrak{b} \le (\omega)$, כלומר, $\mathfrak{c} + \mathfrak{q} \le \mathfrak{c}$, סתירה. לפי משפט 11.7, יש $x \in F^\times$ כך ש־$\omega_1 = x\omega$. מתקיים $x\omega = \omega_1 \in \Omega(\mathfrak{a})$, לכן לפי משפט 11.9, $\mathfrak{a} \le (x\omega) = (x) + (\omega)$, כלומר, $\mathfrak{c} + \mathfrak{p} \le (x) + \mathfrak{c}$. מכאן $0 < \mathfrak{p} \le (x)$. בפרט, $\deg(x) > 0$, בסתירה למשפט 8.8. ∎

12. משפט רימן־רוך

יהי F שדה פונקציות אלגבריות במשתנה אחד מעל K. יהי g הגזע שלו.

משפט 12.1 (רימן־רוך): *יהי $\mathfrak{w} \in W$ מחלק קנוני ויהי $\mathfrak{a}$ מחלק. אז*

(א) $\delta(\mathfrak{a}) = \dim(\mathfrak{w} - \mathfrak{a})$.

(ב) $\dim \mathfrak{a} = \deg \mathfrak{a} + 1 - g + \dim(\mathfrak{w} - \mathfrak{a})$.

הוכחה: (א) כזכור, $\mathfrak{w} = (\omega)$, באשר $0 \neq \omega \in \Omega$. ההעתקה $T\colon F \to \Omega$ על ידי $x \mapsto x\omega$ הינה לינארית מעל K (ואפילו מעל F) וחד חד ערכית. מתקיים

$$x \in \mathcal{L}(\mathfrak{w} - \mathfrak{a}) \Leftrightarrow (x) + (\omega) - \mathfrak{a} \geq 0 \Leftrightarrow (x\omega) \geq \mathfrak{a} \Leftrightarrow x\omega \in \Omega(\mathfrak{a}).$$

לכן T מעתיקה את $T\big(\mathcal{L}(\mathfrak{w} - \mathfrak{a})\big)$ לתוך $\Omega(\mathfrak{a})$. כמו כן, לפי משפט 11.7, כל דיפרנציאל, בפרט כל איבר ב־$\Omega(\mathfrak{a})$, הוא מהצורה $x\omega$, עבור איזה $x \in F$. לכן $T\big(\mathcal{L}(\mathfrak{w} - \mathfrak{a})\big) = \Omega(\mathfrak{a})$. מכאן שוויון הממדים (א).

(ב) הצב (א) במסקנה 11.4. ∎

מסקנה 12.2: *יהי $\mathfrak{w}$ מחלק קנוני, ויהי $\mathfrak{a}$ מחלק.*

(א) *אם $\mathfrak{a}$ ראשי אז* $\dim \mathfrak{a} = 1$, $\deg \mathfrak{a} = 0$. *בפרט* $\dim 0 = 1$, $\deg 0 = 0$.

(ב) $\dim \mathfrak{w} = g$, $\deg \mathfrak{w} = 2g - 2$.

(ג) *אם* $\deg \mathfrak{a} < 0$ *אז* $\dim \mathfrak{a} = 0$.

(ד) *אם* $\deg \mathfrak{a} = 0$ *ו־$\mathfrak{a}$ אינו ראשי אז* $\dim \mathfrak{a} = 0$.

(ה) *אם* $\deg \mathfrak{a} > 2g - 2$ *אז* $\dim \mathfrak{a} = \deg \mathfrak{a} + 1 - g$.

(ו) *אם* $\deg \mathfrak{a} = 2g - 2$ *ו־$\mathfrak{a}$ אינו קנוני אז* $\dim \mathfrak{a} = g - 1$.

הוכחה: (א) יהי $x \in F$. אז $\deg(x) = 0$ לפי משפט 8.8. אם $x \in K$ אז $(x) = 0$ ו־$\mathcal{L}(0) = K$, לכן הטענה ברורה. אם $x \in F^\times$ אז $x\mathcal{L}\big((x)\big) = \mathcal{L}(0)$ לפי טענה 7.2(ד) (עם $S = \mathbb{P}$), לכן $\dim(x) = \dim 0 = 1$.

(ב) נציב $\mathfrak{a} = 0$ ו־$\mathfrak{a} = \mathfrak{w}$ במשפט רימן־רוך: $1 = 0 + 1 - g + \dim \mathfrak{w}$, $\dim \mathfrak{w} = \deg \mathfrak{w} + 1 - g + 1$. מהמשוואה הראשונה, $\dim \mathfrak{w} = g$, מהשניה $\deg \mathfrak{w} = 2g - 2$.

(ג), (ד) נניח $\dim \mathfrak{a} > 0$; צריך להוכיח כי $\deg \mathfrak{a} \geq 0$ ואם $\deg \mathfrak{a} = 0$ אז $\mathfrak{a}$ ראשי. לפי הנתון יש $x \in F^\times$ כך ש־$(x) + \mathfrak{a} \geq 0$. מכאן $\deg \mathfrak{a} = \deg\big((x) + \mathfrak{a}\big) \geq 0$ ואם $\deg \mathfrak{a} = 0$ אז $(x) + \mathfrak{a} = 0$, כלומר $\mathfrak{a} = -(x) = (x^{-1})$ ראשי.

(ה) אם $\deg \mathfrak{a} > 2g - 2$ אז $\deg(\mathfrak{w} - \mathfrak{a}) = \deg \mathfrak{w} - \deg \mathfrak{a} < 0$ לפי (ב). לכן $\dim(\mathfrak{w} - \mathfrak{a}) = 0$ לפי (ג), ומכאן $\dim \mathfrak{a} = \deg \mathfrak{a} + 1 - g$ לפי משפט רימן־רוך.

(ו) אם $\deg \mathfrak{a} = 2g - 2$ אז $\deg(\mathfrak{w} - \mathfrak{a}) = \deg \mathfrak{w} - \deg \mathfrak{a} = 0$ לפי (ב). לכן, לפי (ד) $\dim(\mathfrak{w} - \mathfrak{a}) = 0$ או $\mathfrak{w} - \mathfrak{a} = (x)$ עבור איזה $x \in F^\times$. במקרה הראשון $\dim \mathfrak{a} = 2g - 2 + 1 - g + 0 = g - 1$ ובמקרה השני $\mathfrak{a} = \mathfrak{w} - (x)$ קנוני. ∎

תרגיל 12.3: *יהיו $\mathfrak{a},\mathfrak{b}$ מחלקים.*

(א) *אם $\mathfrak{a},\mathfrak{b}$ באותה מחלקה של מחלקים אז $\deg\mathfrak{a}=\deg\mathfrak{b}$, $\dim\mathfrak{a}=\dim\mathfrak{b}$.*

(ב) $\dim\mathfrak{b}\le\max(0,\deg\mathfrak{b}+1)$.

(ג) *יהי $g'\in\mathbb{Z}$ ויהי $\mathfrak{w}'$ מחלק כך שלכל מחלק $\mathfrak{a}$ מתקיים $\dim\mathfrak{a}=\deg\mathfrak{a}+1-g'+\dim(\mathfrak{w}'-\mathfrak{a})$. אזי $g'=g$ ו־ $\mathfrak{w}'$ הוא מחלק קנוני.*

הוכחה: (א) נניח $\mathfrak{b}=\mathfrak{a}+(x)$, באשר $x\in F^\times$. אז $\deg(x)=0$, לכן $\deg\mathfrak{a}=\deg\mathfrak{b}$. לפי טענה 7.2(ד), $\mathcal{L}(\mathfrak{a})=x\mathcal{L}(\mathfrak{b})$, לכן $\mathcal{L}(\mathfrak{a})\cong\mathcal{L}(\mathfrak{b})$, ולכן $\dim\mathfrak{a}=\dim\mathfrak{b}$.

(ב) אם $\dim\mathfrak{b}=0$, זה ברור. אחרת יש $x\in F^\times$ כך ש־$(x)+\mathfrak{b}\ge 0$. לפי (א) אפשר להחליף את $\mathfrak{b}$ ב־$\mathfrak{b}+(x)$. לכן בלי הגבלת הכלליות $\mathfrak{b}\ge 0$. לפי מסקנה 7.6, $\deg\mathfrak{b}-\dim\mathfrak{b}\le\deg 0-\dim 0=0-1$. מכאן $\dim\mathfrak{b}\le\deg\mathfrak{b}+1$.

(ג) נציב $\mathfrak{a}$ כך ש־$\deg\mathfrak{a}>>0$. אז לפי משפט 12.2 $\dim\mathfrak{a}=\deg\mathfrak{a}+1-g$ ואילו $\deg(\mathfrak{w}'-\mathfrak{a})<0$, לכן $\dim(\mathfrak{w}'-\mathfrak{a})=0$. נציב זאת בנתון ונקבל $g=g'$.

נציב $\mathfrak{a}=0$. אז מהנתון, $1=\dim 0=0+1-g+\dim(\mathfrak{w}'-0)$ נקבל $\dim\mathfrak{w}'=g$.

נציב $\mathfrak{a}=\mathfrak{w}'$. אז מהנתון, $\dim\mathfrak{w}'=\deg\mathfrak{w}'+1-g+\dim(0)$, כלומר, $g=\deg\mathfrak{w}'+1-g+1$.

מכאן $\deg\mathfrak{w}'=2g-2$. לפי משפט 12.2(ו), $\mathfrak{w}'$ הוא מחלק קנוני. ∎

משפט 12.4 (משפט הקירוב החזק): *תהי $S\subseteq\mathbb{P}$ סופית ויהי $\mathfrak{q}\in\mathbb{P}\smallsetminus S$. לכל $\mathfrak{p}\in S$ יהיו נתונים $x_\mathfrak{p}\in F$ ו־$m_\mathfrak{p}\in\mathbb{Z}$. אז יש $x\in F$ שמקיים $v_\mathfrak{p}(x-x_\mathfrak{p})\ge m_\mathfrak{p}$ לכל $\mathfrak{p}\in S$ ו־$v_\mathfrak{p}(x)\ge 0$ לכל $\mathfrak{p}\notin S\cup\{\mathfrak{q}\}$.*

הוכחה: נסמן $\mathfrak{a}=m\mathfrak{q}-\sum_{\mathfrak{p}\in S}m_\mathfrak{p}\mathfrak{p}$, באשר $m\in\mathbb{N}$ גדול מספיק, כך ש־$\deg\mathfrak{a}>2g-2$. אז לפי מסקנה 12.2(ה), $\deg\mathfrak{a}-\dim\mathfrak{a}=g-1$. לכן לפי מסקנה 10.6, $\Lambda(\mathfrak{a})+F=\mathbb{A}$.

נגדיר $\alpha\in\mathbb{A}$ על ידי $\alpha_\mathfrak{p}=\begin{cases}x_\mathfrak{p} & \mathfrak{p}\in S\\ 0 & \mathfrak{p}\notin S\end{cases}$. אז יש $x\in F$ כך ש־$x-\alpha\in\Lambda(\mathfrak{a})$. כלומר, $v_\mathfrak{p}(x-x_\mathfrak{p})\ge v_\mathfrak{p}(-\mathfrak{a})$ לכל $\mathfrak{p}\in\mathbb{P}$. לכן x מקיים את דרישות המשפט. ∎

תרגיל 12.5: *הראה שבתנאים של המשפט אפשר לדרוש $v_\mathfrak{p}(x-x_\mathfrak{p})=m_\mathfrak{p}$ במקום $v_\mathfrak{p}(x-x_\mathfrak{p})\ge m_\mathfrak{p}$ לכל $\mathfrak{p}\in S$.*

תרגיל 12.6: *הראה שאם נחליף במשפט את התנאי $\mathfrak{p}\notin S\cup\{\mathfrak{q}\}$ ב־ $\mathfrak{p}\notin S$, המשפט לא יהיה נכון.*

13. הקשר למשטחי רימן

פרק זה הוא רק לשם ידיעה כללית. ההגדרות בו הן חלקיות בלבד והמשפטים יובאו ללא הוכחות.

הגדרה 13.1: **משטח רימן** S הוא יריעה מרוכבת קשירה בעלת מימד 1; אנחנו גם נניח שהוא **קומפקטי**. כלומר, $S=\bigcup_{i=1}^{k} V_i$ הוא מרחב טופולוגי האוסדורף, באשר V_i קבוצות פתוחות, ולכל i יש הומיאומורפיזם $\varphi_i\colon V_i \to U_i \subseteq \mathbb{C}$ על קבוצה פתוחה U_i ב־$\mathbb{C}$, כך שלכל $1 \le i,j \le k$ ההעתקה $\varphi_1\circ\varphi_2^{-1}\colon \varphi_2(V_1\cap V_2) \to \varphi_1(V_1\cap V_2)$ היא הולומורפית. בנוסף לכך, בגלל ש־S קומפקטי, "אין לו שפה", כלומר, S מכיל גם את השפה של כל V_i (כל נקודה בה מוכלת באיזה V_j אחר).

(כמובן, כיסויים שונים מהסוג $\{V_i\}$ לעיל יכולים להגדיר אותו משטח רימן –יש יחס שקילות על הכיסויים .)

∎

דוגמאות 13.2: ספֵרת רימן $\mathbb{P}^1$, טוֹרוּס ("פני צמיג"), הדבקת n ספֵרות לאורך מסלול נתון (הסבר בעל פה...). ∎

משפט 13.3: *כל משטח רימן הומיאומורפי לספֵרת רימן עם g ידיות, באשר $g \ge 0$. המספר g הוא שמורה של המשטח, נקרא* ***הגזע*** *של המשטח. שני משטחי רימן הומיאומורפיים אם ורק אם הם בעלי אותו גזע.*

כמובן, משטחי רימן הומיאומורפיים אינם בהכרח שווים.

הגדרה 13.4: כיסוי של משטחי רימן. העתקה של משטחי רימן $f\colon S' \to S$ היא **כיסוי**, אם היא על ומהצורה הבאה: נניח

- $S=\bigcup_{i=1}^{k} V_i$, עם ההעתקות $\varphi_i\colon V_i \to U_i \subseteq \mathbb{C}$, כאשר כל U_i הוא עיגול היחידה סביב הראשית,
- ו־$S'=\bigcup_{j=1}^{m} U_j'$, עם ההעתקות $\varphi_i'\colon V_i' \to U_i' \subseteq \mathbb{C}$, כאשר כל V_j' הוא עיגול היחידה סביב הראשית,

אז לכל $x' \in S'$ יש i,j כך ש־$x' \in V_j'$ וקיים התרשים החילופי הבא:

$$\begin{tikzcd} V_j' \arrow[r, "\varphi_j'"] \arrow[d, "f|_{V_j'}"'] & U_j' \arrow[d, "f_{ij}"] \\ V_i \arrow[r, "\varphi_i"'] & U_i \end{tikzcd}$$

ו־f_{ij} היא ההעתקה $z \mapsto z^e$ עבור איזה $e=e(x') \in \mathbb{N}$.

מסתבר שיש $n \in \mathbb{N}$, שייקרא **המעלה** של הכיסוי, כך שעבור כמעט כל $x \in S$ הסיב $f^{-1}(\{x\})$ של x הוא בן n איברים ו־$e(x')=1$ לכל x' בסיב. עבור מספר סופי של $x \in S$ האחרים הסיב הוא קטן יותר. ∎

דוגמאות 13.5: הדבקת n ספֵרות היא כיסוי של ספרה. ∎

הגדרה 13.6: פונקציה מירומורפית. תהי $U \subseteq \mathbb{C}$ קבוצה פתוחה. העתקה $h\colon U \to \mathbb{C}\cup\{\infty\}$ נקראת מירומורפית, אם היא מנה של שתי פונקציות הולומורפיות.

יהי S משטח רימן נתון על ידי $S=\bigcup_{i=1}^n V_i$ והעתקות $\{\varphi_i\colon V_i\to U_i\}_{i=1}^k$. העתקה $h\colon S\to \mathbb{C}\cup\{\infty\}$ נקראת **מירומורפית**, אם $h\circ\varphi_i^{-1}\colon U_i\to\mathbb{C}\cup\{\infty\}$ מירומורפיות, לכל $1\le i\le k$. ∎

משפט 13.7: *יהי S משטח רימן. קבוצת הפונקציות המירומורפיות $\mathcal{M}(S)$ על S משטח רימן היא שדה,* ***שדה הפונקציות המירומורפיות על*** *S. הוא שדה פונקציות אלגבריות במשתנה אחד מעל $\mathbb{C}$. הגזע של $\mathcal{M}(S)$ שווה לגזע של S.*

דוגמה 13.7: שדה הפונקציות המירומורפיות על ספרת רימן $\mathbb{P}^1$ הוא שדה הפונקציות הרציונליות $\mathbb{C}(t)$ במשתנה אחד t מעל $\mathbb{C}$. ∎

יהי $f\colon S'\to S$ כיסוי של משטחי רימן. אם h פונקציה מירומורפית על S, אז $h\circ f$ היא פונקציה מירומורפית על S'. לכן $h\mapsto h\circ f$ היא העתקה $\mathcal{M}(f)\colon\mathcal{M}(S)\to\mathcal{M}(S')$. העתקה זו היא הומומורפיזם של שדות. בפרט היא חד חד ערכית, ולכן אפשר לזהות אותה עם הכלה של שדות. המעלה של ההרחבה שווה למעלת הכיסוי f.

באופן זה מגדירים פונקטור מהקטגוריה של של משטחי רימן, עם העתקות הכיסויים ביניהם, לתוך הקטגוריה של שדות, עם הכלות ביניהם.

משפט 13.8: *הפונקטור $S\mapsto\mathcal{M}(S)$ הוא שקילות קטגוריות.*

בפרט, אם $S\to\mathbb{P}^1$ הוא כיסוי ממעלה n של ספרת רימן, אז שדה הפונקציות המירומורפיות F על S הוא שדה פונקציות אלגבריות במשתנה אחד מעל $\mathbb{C}$.

להיפך, אם $F/\mathbb{C}$ שדה פונקציות אלגבריות במשתנה אחד אז יש משטח רימן S וכיסוי $S\to\mathbb{P}^1$ כך ש־F הוא שדה הפונקציות המירומורפיות על S. (כקבוצה, S היא $\mathbb{P}(F)$, קבוצת המחלקים הראשוניים על F.)

14. שדה הפונקציות הרציונליות

יהי K שדה ויהי $F=K(t)$, באשר t טרנסצנדנטי מעל K. בפרק 6 הופיע:

תרגיל 6.3: *$F=K(t)$ הוא שדה פונקציות אלגבריות במשתנה אחד מעל K.*

ניישם את המושגים שלמדנו למקרה זה.

לפי משפט 2.2 מחלקים ראשוניים של $K(t)/K$ הם משני סוגים:

(א) מחלק אשר מתאים לפולינום אי פריק מתוקן $p=p(t)\in K[t]$; נסמנו $\hat{p}$. האתר המתאים הוא ההרחבה של העתקת המנה $K[t]\to K[t]/pK[t]$ ושדה השאריות הוא $K[t]/pK[t]$. לכן $\deg\hat{p}=\deg p$.

(ב) מחלק האינסוף $\mathfrak{p}_\infty$. האתר המתאים הוא ההרחבה של ההומומורפיזם $K[t^{-1}]\to K$ על ידי $t^{-1}\mapsto 0$ ושדה השאריות הוא K. לכן $\deg\mathfrak{p}_\infty=1$.

לכל פונקציה רציונלית $0\neq f\in K(t)$ יש הצגה יחידה

$$f=c\prod_p p^{n_p},\qquad c\in K^\times,\ n_p\in\mathbb{Z} \tag{1}$$

כאשר $n_p=0$ כמעט לכל p. אז $v_p(f)=n_p$ לכל p ו־$v_\infty(f)=-\deg f$, כפי שראינו בפרק 2. לכן

$$(f)=\sum_p n_p p-(\deg f)\mathfrak{p}_\infty. \tag{2}$$

(נשים לב שמתקיים $\deg(f)=\sum_p n_p\deg p-\deg f=0$.)

נחשב את הגזע g. יהי $n\in\mathbb{N}$. יהי f נתון על ידי (1). אז

$$f\in\mathcal{L}(n\mathfrak{p}_\infty)\Leftrightarrow(f)\geq -n\mathfrak{p}_\infty\Leftrightarrow n_p\geq 0 \text{ לכל } p,-\deg f\geq -n\Leftrightarrow f\in K[t],\deg f\leq n$$

לכן $1,t,\ldots,t^n$ בסיס של $\mathcal{L}(n\mathfrak{p}_\infty)$ מעל K. מכאן $\dim n\mathfrak{p}_\infty=n+1$. כמובן, $\deg n\mathfrak{p}_\infty=n$. אם ניקח $n>2g-2$ אז לפי מסקנה 12.2(ה), $n+1=n+1-g$. מכאן $g=0$.

כמו כן, לפי מסקנה 12.2, אם $\mathfrak{w}$ מחלק קנוני, אז $\deg\mathfrak{w}=2g-2=-2$ ואם $\deg\mathfrak{a}=-2$ ו־$\mathfrak{a}$ אינו קנוני אז $\dim\mathfrak{a}=g-1=-1$, שלא יתכן. בכך הוכחנו:

משפט 14.1: *הגזע של שדה הפונקציות הרציונליות הוא $g=0$. כל מחלק ממעלה -2 הוא קנוני.*

תרגיל 14.2: *הוכח שכל מחלק ממעלה 0 של $K(t)/K$ הוא ראשי. הסק שחבורת מחלקות המחלקים איזומורפית ל־$\mathbb{Z}$.*

תרגיל 14.3: *יהי $\mathfrak{a}$ מחלק של $K(t)/K$. אז $\dim\mathfrak{a}=\max(0,\deg\mathfrak{a}+1)$.*

תרגיל 14.4: *יהי $0\neq f\in K[t]$ פולינום. אז $\deg(f)_0=\deg f$.*

15. שדות פונקציות ממעלה 2 מעל שדות פונקציות רציונליות

יהי F/K שדה פונקציות אלגבריות במשתנה אחד.

נתחיל בהכנות כלליות.

שני מחלקים $\mathfrak{a}, \mathfrak{b}$ של F/K הם **זרים** אם אין מחלק ראשוני $\mathfrak{p}$ כך ש־$v_\mathfrak{p}(\mathfrak{a}) \neq 0$ וגם $v_\mathfrak{p}(\mathfrak{b}) \neq 0$.

למשל, אם $x \in F^\times$, אז $(x)_0, (x)_\infty$ זרים.

למה 15.1: *יהי $x \in F \setminus K$ ויהי $0 \neq f \in K[X]$. אז*

(א) $\big(f(x)\big)_0, (x)_\infty$ *זרים.*

(ב) $\big(f(x)\big)_\infty = (\deg f) \cdot (x)_\infty$.

הוכחה: אם $0 \neq f \in K$, אז $\deg f = 0$ ו־$f(x) = f \in K^\times$, לכן $\big(f(x)\big) = \big(f(x)\big)_0 = \big(f(x)\big)_\infty = 0$.
לכן טענות (א), (ב) ברורות.

אחרת $f(x) = \sum_{i=0}^n c_i x^i$, באשר $n = \deg f \geq 1$ ו־$c_n \neq 0$. יהי $\mathfrak{p} \in \mathbb{P}$. אז $v_\mathfrak{p}(c_i x^i) = i v_\mathfrak{p}(x)$ לכל $0 \leq i \leq n$ ולכל $0 \neq c_i \in K$. לכן:

אם $v_\mathfrak{p}(x) \geq 0$ אז $v_\mathfrak{p}\big(f(x)\big) \geq \min_{i:c_i \neq 0} i v_\mathfrak{p}(x) \geq 0$, לפי טענה 1.10(ד).

אם $v_\mathfrak{p}(x) < 0$ אז $v_\mathfrak{p}\big(f(x)\big) = \min_{i:c_i \neq 0} i v_\mathfrak{p}(x) = n v_\mathfrak{p}(x) < 0$, לפי טענה 1.10(ג). מכאן שתי הטענות, (א), (ב). (בדקו!) ∎

למה 15.2: *יהי $x \in F \setminus K$ ויהי $0 \neq r = \frac{f_1(x)}{f_2(x)} \in K(x)$, באשר $f_1, f_2 \in K[X]$ זרים זה לזה. אז*

(א) $(r) = \big(f_1(x)\big)_0 - \big(f_2(x)\big)_0 + (\deg f_2 - \deg f_1) \cdot (x)_\infty$.

(ב) *המחלקים* $(x)_\infty, \big(f_1(x)\big)_0, \big(f_2(x)\big)_0$ *זרים זה לזה בזוגות.*

(ג) *יהי $n \in \mathbb{Z}$. אז $r \in \mathcal{L}\big(n(x)_\infty\big)$ אם ורק אם f_2 קבוע ו־$\deg f_1 \leq n$.*

(ד) $\big[K(x) : K(r)\big] = \max(\deg f_1, \deg f_2)$.

(ה) $K(x) = K(r)$ *אם ורק אם* $r = \frac{ax+b}{cx+d}$, *באשר* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$.

הוכחה: (א) לפי למה 15.1(ב),

$$(r) = \big(f_1(x)\big) - \big(f_2(x)\big) = \Big(\big(f_1(x)\big)_0 - \big(f_1(x)\big)_\infty\Big) - \Big(\big(f_2(x)\big)_0 - \big(f_2(x)\big)_\infty\Big) =$$
$$= \big(f_1(x)\big)_0 - \big(f_2(x)\big)_0 + (\deg f_2 - \deg f_1) \cdot (x)_\infty$$

(ב) יהי $1 \leq i \leq 2$. לפי למה 15.1(א), $(x)_\infty, \big(f_i(x)\big)_0$ זרים. בפרט, אם $v_\mathfrak{p}\big(f_i(x)\big) > 0$ אז $v_\mathfrak{p}(x) \geq 0$ ולכן, לפי למה 15.1(ב), $v_\mathfrak{p}\big(g(x)\big) \geq 0$ לכל $g \in K[X]$. כיוון ש־f_1, f_2 זרים, יש פולינומים $g_1, g_2 \in K[X]$ כך ש־$g_1(x)f_1(x) + g_2(x)f_2(x) = 1$. לכן אם $v_\mathfrak{p}\big(f_1(x)\big), v_\mathfrak{p}\big(f_2(x)\big) > 0$ אז $v_\mathfrak{p}(1) > 0$, סתירה.

(ג) לפי ההצגה של (r) בסעיף (א) ולפי הזרות בסעיף (ב), $\Leftrightarrow r \in \mathcal{L}\big(n(x)_\infty\big)$

$$(r) + n(x)_\infty \geq 0 \Leftrightarrow \big(f_1(x)\big)_0 - \big(f_2(x)\big)_0 + (\deg f_2 - \deg f_1 + n) \cdot (x)_\infty \geq 0$$

$$\Leftrightarrow \big(f_2(x)\big)_0 = 0,\ \deg f_2 - \deg f_1 + n \geq 0 \Leftrightarrow f_2 \in K^\times,\ n \geq \deg f_1$$

(ד) בלי הגבלת הכלליות $F = K(x)$. בלי הגבלת הכלליות $\deg f_1 \leq \deg f_2$, אחרת נחליף את r ב-r^{-1}.

לפי (א), (ב), $(r)_\infty = \big(f_2(x)\big)_0$. לכן לפי לפי משפט 8.8 ולמה 15.1(ב),

$$[F : K(r)] = \deg(r)_\infty = \deg\big(f_2(x)\big)_0 = \deg\big(f_2(x)\big)_\infty = \deg f_2 = \max(\deg f_1, \deg f_2).$$

(ה) לפי (ד), $K(x) = K(r)$ אם ורק אם $\max(\deg f_1, \deg f_2) = 1$, כלומר, $f_2 = cx + d$, $f_1 = ax + b$, באשר $a, b, c, d \in K$, ו-a, c לא שניהם אפס.

בתנאים האלה, הפולינומים f_1, f_2 זרים אם ורק אם אף אחד מהם אינו כפולה של השני באיבר של $K^\times$, כלומר, $(a, b), (c, d)$ אינם תלויים לינארית מעל K, כלומר, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ הפיכה. ∎

תרגיל 15.3: *יהיו $F_1/K_1, F_2/K_2$ שני שדות פונקציות אלגבריות במשתנה אחד. יהיו $\mathbb{P}_1, \mathbb{P}_2$ קבוצות המחלקים הראשוניים ו-$\mathcal{D}_1, \mathcal{D}_2$ חבורות המחלקים של שני השדות, בהתאמה. יהי $\sigma\colon F_1 \to F_2$ איזומורפיזם של שדות כך ש-$\sigma(K_1) = K_2$.*

(א) *הראו שיש התאמה חד חד ערכית בין $\sigma\colon \mathbb{P}_1 \to \mathbb{P}_2$ הנתונה על יד $v_{\sigma\mathfrak{p}}(x) = v_\mathfrak{p}\big(\sigma^{-1}(x)\big)$ (או, באופן שקול, על ידי $\mathcal{O}_{\sigma\mathfrak{p}} = \sigma(\mathcal{O}_\mathfrak{p})$).*

(ב) *הראו שההתאמה $\mathfrak{p} \mapsto \sigma\mathfrak{p}$ ניתנת להרחבה לאיזומורפיזם חבורות $\sigma\colon \mathcal{D}_1 \to \mathcal{D}_2$.*

(ג) *הראו שמתקיים $\big(\sigma(x)\big) = \sigma\big((x)\big)$ ו-$\big(\sigma(x)\big)_\infty = \sigma\big((x)_\infty\big)$ לכל $x \in F_1$.*

(ד) *הראו שמתקיים $\mathcal{L}(\sigma\mathfrak{a}) = \sigma\big(\mathcal{L}(\mathfrak{a})\big)$ לכל $\mathfrak{a} \in \mathcal{D}_1$.*

מעתה ועד סוף הפרק נניח כי $\operatorname{char} K \neq 2$ ויש $x \in F \smallsetminus K$ כך ש-$[F : K(x)] = 2$.

למה 15.4: *נניח כי $\operatorname{char} K \neq 2$ ויש $x \in F \smallsetminus K$ כך ש-$[F : K(x)] = 2$. אז יש $y \in F$ כך ש-$F = K(x, y)$ ומתקיים $y^2 = d(x)$, באשר $d \in K[X]$ פולינום ממעלה ≥ 1 שאין לו גורמים אי פריקים מרובים.*

הוכחה: יש $y \in F$ כך ש-$F = K(x, y)$ ויש $b, c \in K(x)$ כך ש-y שרש של משוואה ריבועית $y^2 + by + c = 0$. השלמה לריבוע נותנת

$$\Big(y + \frac{b}{2}\Big)^2 = \frac{b^2}{4} - c.$$

לכן, אם נחליף את y ב-$y + \frac{b}{2}$, נוכל להניח שיש $d \in K(x)$ כך ש-$y^2 = d$, נאמר, $d = \frac{f_1(x)}{f_2(x)}$, באשר $f_2 \neq 0$. בלי הגבלת הכלליות $f_2 = 1$ אחרת נחליף את y ב-$f_2(x)y$.

נשים לב ש-$\deg d \geq 1$, אחרת $y^2 = d \in K$, ובפרט y אלגברי מעל K ולכן $y \in K$, בסתירה ל-$[K(x, y) : K(x)] = 2$. יהי $d = p_1^{m_1} \cdots p_r^{m_r}$ פירוק של d לפולינומים אי פריקים, $m_i \geq 1$. בלי הגבלת הכלליות $m_i = 1$ לכל i (או $m_i = 0$ אבל אז נשמיט את p_i), אחרת נחלק את y ב-$\prod_i p_i^{\lfloor \frac{m_i}{2} \rfloor} \in K(x)$. ∎

למה 15.5: *בתנאים של הלמה הקודמת יהי* $m = \deg d$. *אז* $\dim n(x)_\infty = \lfloor 2n+2-\frac{m}{2}\rfloor = 2n+2-\lceil \frac{m}{2}\rceil$ *לכל* $n \in \mathbb{N}$.

הוכחה: כיוון ש־$\mathrm{char}\ K(x) \neq 2$ ו־$[F : K(x)] = 2$, ההרחבה $F/K(x)$ פרידה; לכן היא הרחבת גלואה. תהי $\{1,\sigma\}$ חבורת גלואה שלה. אז $\sigma(y) = -y$. כיוון ש־$\sigma(x) = x$, מתקיים $\sigma\Big(\mathcal{L}\big(n(x)_\infty\big)\Big) = \mathcal{L}\big(n(x)_\infty\big)$.

לכל $z \in F$ יש הצגה יחידה $z = f(x) + g(x)y$, באשר $f(x), g(x) \in K(x)$. בהצגה זו $\sigma(z) = f(x) - g(x)y$. אם $z \in \mathcal{L}\big(n(x)_\infty\big)$, אז, לפי תרגיל 15.3 גם $\sigma(z) \in \mathcal{L}\big(n(x)_\infty\big)$. לכן

$$f(x) = \frac{1}{2}\big(z+\sigma(z)\big) \in \mathcal{L}\big(n(x)_\infty\big)\ ,$$
$$f^2(x) - d(x)g^2(x) = z\cdot\sigma(z) \in \mathcal{L}\big(n(x)_\infty + n(x)_\infty\big) = \mathcal{L}\big(2n(x)_\infty\big).$$

לפי למה 15.2(ג), $f \in K[X]$ פולינום ממעלה $\deg f \leq n$ ו־$f^2 - dg^2 \in K[X]$ ממעלה $\geq 2n$. בפרט $dg^2 \in K[X]$ ו־$\deg dg^2 \leq 2n$. ומכאן, כיוון של־d אין גורמים אי פריקים מרובים, $g \in K[X]$ ו־$\deg g \leq n - \frac{m}{2}$.

להיפך, אם $f, g \in K[X]$, $\deg f \leq n\ ,\ \deg g \leq n - \frac{m}{2}$, אז $z = f(x)+g(x)y \in \mathcal{L}\big(n(x)_\infty\big)$:

$$\big(f(x)\big) = \big(f(x)\big)_0 - \big(f(x)\big)_\infty = \big(f(x)\big)_0 - (\deg f)(x)_\infty \geq -n(x)_\infty$$
$$\big(g(x)y\big) = \big(g(x)\big)_0 - \big(g(x)\big)_\infty + \frac{1}{2}(y^2)_0 - \frac{1}{2}(y^2)_\infty \geq -\big(g(x)\big)_\infty - \frac{1}{2}(y^2)_\infty =$$
$$= -(\deg g)(x)_\infty - \frac{1}{2}(\deg d)(x)_\infty \geq -(n-\frac{m}{2})(x)_\infty - \frac{m}{2}(x)_\infty = -n(x)_\infty$$

לכן $z = f(x)+g(x)y \in \mathcal{L}\big(n(x)_\infty\big)$.

לכן $\mathcal{L}\big(n(x)_\infty\big)$ נפרש מעל K על ידי $\{x^i |\ 0 \leq i \leq n\}\bigcup\{x^iy |\ 0 \leq i \leq n - \frac{m}{2}\}$. לפי למה 8.6(א) קבוצה זו בלתי תלויה לינארית מעל K. לכן $\dim n(x)_\infty$ הוא מספר איבריה, $n+1+\lfloor n+1-\frac{m}{2}\rfloor$. ∎

לפי משפט 8.8, $\deg(x)_\infty = [F : K(x)] = 2$. אם n גדול מספיק, אז $\dim n(x)_\infty = \deg n(x)_\infty + 1 - g$, כלומר, $2n+2-\lceil\frac{m}{2}\rceil = 2n+1-g$. מכאן $g = \lceil\frac{m}{2}\rceil - 1$, כלומר

משפט 15.6: *בתנאים לעיל הגזע של* F/K *הוא* $g = \begin{cases} \frac{m-2}{2} & m \text{ זוגי} \\ \frac{m-1}{2} & m \text{ אי זוגי} \end{cases}$. *כלומר,* $g = 0$ *עבור* $m = 1, 2$, $g = 1$ *עבור* $m = 3, 4$, $g = 2$ *עבור* $m = 5, 6$, *וכן הלאה.*

הגדרה 15.7: בתנאים לעיל אם $g = 1$ ול־F/K יש מחלק ראשוני ממעלה 1, F נקרא **שדה פונקציות אליפטיות** מעל K. אם $g \geq 2$, F נקרא **שדה פונקציות היפֶּרְאֶליפטיות** מעל K.

תרגיל 15.8: *מצא את המחלקים הקנוניים של* F/K *בתנאים לעיל.*

תרגיל 15.9: *יהי* K *שדה,* $\mathrm{char}\ K \neq 2$, *יהי* x *טרנסצנדנטי מעל* K, *ויהי* $d \in K[X]$ *חפשי מריבוע, ממעלה* $m \geq 1$. *יהי* $F = K(x,y)$ *באשר* $y^2 = d(x)$. *הוכיחו ש־*F/K *הוא שדה פונקציות אלגבריות במשתנה אחד.*

הוכחה: צריך להוכיח ש־K סגור אלגברית ב־F.

נניח בשלילה שיש $\alpha \in F \setminus K$ אלגברי מעל K. לפי תרגיל 6.7, הפולינום האי פריק של α מעל K הינו אי פריק מעל $K(x)$. כיוון שיש לו שורש בהרחבה ריבועית F של $K(x)$ ואין לו שורש ב־K, הוא בעל מעלה 2. בלי הגבלת הכלליות (על ידי השלמה לריבוע ־ וכאן משתמשים בכך ש־$\mathrm{char}\ K \neq 2$) $a := \alpha^2 \in K$. אז $X^2 - a$ הוא הפולינום האי פריק של α מעל K. כאמור, הוא נשאר אי פריק גם מעל $K(x)$. לכן שורשו $\alpha \in F$ יוצר הרחבה ממעלה 2 של $K(x)$ מוכלת ב־F. מכאן ש־$F = K(x)(\alpha)$. בפרט $1, \alpha$ הוא בסיס של F מעל $K(x)$.

כעת, $y \in K(x)(\alpha)$, לכן יש $f(x), g(x) \in K(x)$ כך ש־ $y = f(x) + g(x)\alpha$. מכאן

$$d(x) = y^2 = f^2(x) + ag^2(x) + 2f(x)g(x)\alpha.$$

לכן (לפי יחידות ההצגה של וקטור כצירוף לינארי של איברי בסיס) $f(x)g(x) = 0$.

אם $g(x) = 0$ אז $y = f(x) \in K(x)$, סתירה.

אם $f(x) = 0$ אז $d(x) = ag^2(x)$. כיוון ש־$\deg d = m \geq 1$, גם $\deg g \geq 1$. אז d הוא בעל גורמים אי פריקים מרובים, סתירה. ∎

תרגיל 15.10: *מצא את הגזע של F/K כאשר $\mathrm{char}\ K = 2$ וההרחבה $F/K(x)$ ממעלה 2 לא פרידה.*

תרגיל 15.11: *מצא את הגזע של F/K כאשר $\mathrm{char}\ K = 2$ וההרחבה $F/K(x)$ ממעלה 2 פרידה.*

16. שדות בעלי גזע 0

משפט 16.1: *יהי F/K שדה פונקציות בעל גזע $g = 0$. אז F הוא שדה פונקציות רציונליות מעל K או הרחבה ריבועית של שדה כזה. במקרה השני, אם גם $\operatorname{char} K \neq 2$, אז $F = K(t,u)$ באשר $t, u \in F \setminus K$ ו־$u^2 = at^2 + c$, באשר $a, c \in K^\times$.*

הוכחה: יהי $\mathfrak{w}$ מחלק קנוני של F/K. לפי מסקנה 12.2, $\deg \mathfrak{w} = 2g - 2 = -2$. לכן $\deg(-\mathfrak{w}) = 2 > 2g - 2$. מכאן $\dim(-\mathfrak{w}) = \deg(-\mathfrak{w}) + 1 - g = 3$. לכן יש $x, y, z \in \mathcal{L}(-\mathfrak{w})$ בלתי תלויים לינארית מעל K. יהי $t := \frac{x}{y}$. אז $t \in F \setminus K$ ומתקיים

$$(t) = (x) - (y) = \big((x) - \mathfrak{w}\big) - \big((y) - \mathfrak{w}\big), \qquad (x) - \mathfrak{w} \geq 0, \quad (y) - \mathfrak{w} \geq 0,$$

לכן $0 \leq (t)_\infty \leq (y) - \mathfrak{w}$. מכאן $[F : K(t)] = \deg(t)_\infty \leq \deg\big((y) - \mathfrak{w}\big) = -\deg \mathfrak{w} = 2$. לכן $F = K(t)$ שדה פונקציות רציונליות מעל K או הרחבה ריבועית של שדה כזה.

נניח כעת כי $[F : K(t)] = 2$ ו־$\operatorname{char} K \neq 2$. לפי למה 15.4 יש $u \in F$ כך ש־$F = K(t,u)$ ו־$u^2 = d(t)$, באשר $d \in K[X]$ אין לו גורמים אי פריקים מרובים. כיוון ש־$g = 0$, לפי משפט 15.6, $\deg d = 1$ או $\deg d = 2$. לכן $u^2 = at^2 + bt + c$, באשר $a, b, c \in K$ ו־$a \neq 0$ או $b \neq 0$.

אם $a = 0$ אז $t = \frac{u^2 - c}{b} \in K(u)$, לכן $F = K(u)$ הוא שדה פונקציות רציונליות.

אם $a \neq 0$, יהי $t' = t + \alpha$, באשר $\alpha = -\frac{b}{2a} \in K$. אז $K(t) = K(t')$ ומתקיים

$$at^2 + bt + c = a(t' - \alpha)^2 + b(t' - \alpha) + c = a(t')^2 + (b - 2a\alpha)t' + (c + a\alpha^2 - b\alpha) =$$
$$= a(t')^2 + (c + a\alpha^2 - b\alpha).$$

לכן אם נחליף את t ב־t', נקבל את המשוואה המבוקשת. אם $c = 0$ אז $(\frac{u}{t})^2 = a \in K^\times$, לכן $\frac{u}{t} \in F$ אלגברי מעל K, ולכן $\frac{u}{t} \in K$. לכן $F = K(u,t) = K(t)$ שדה פונקציות רציונליות. ∎

איך ניתן להבדיל בין שתי האפשרויות שבמשפט?

משפט 16.2: *יהי F/K שדה פונקציות אלגבריות בעל גזע 0. אז F שדה פונקציות רציונליות מעל K אם ורק אם יש לו מחלק בעל מעלה 1.*

הוכחה: יהי $\mathfrak{a}$ מחלק של F/K ממעלה 1. לפי משפט רימן־רוך (יותר נכון, מסקנה 12.2(ה)) $\dim \mathfrak{a} = \deg \mathfrak{a} + 1 - g = 2$. לכן יש $x, y \in \mathcal{L}(\mathfrak{a})$ בלתי תלויים לינארית מעל K. אחד מהם (לפחות) אינו ב־K, למשל, $x \notin K$. בפרט $x \neq 0$, כך ש־(x) מוגדר. בלי הגבלת הכלליות $\mathfrak{a} \geq 0$, אחרת נחליף את $\mathfrak{a}$ במחלק $\mathfrak{a}' = (x) + \mathfrak{a} \geq 0$, בעל אותה מעלה כמו של $\mathfrak{a}$. אז $(x)_0 - (x)_\infty + \mathfrak{a} = (x) + \mathfrak{a} \geq 0$, כלומר, $(x)_\infty \leq (x)_0 + \mathfrak{a}$. כיוון ש־$(x)_0, (x)_\infty$ זרים, $(x)_\infty \leq \mathfrak{a}$. בפרט $\deg(x)_\infty \leq 1$. כיוון ש־$x \notin K$, לא יתכן

$\deg(x)_\infty = 0$, ולכן $\deg(x)_\infty = 1$. לכן $[F : K(x)] = \deg(x)_\infty = 1$, כלומר, $F = K(x)$ הוא שדה פונקציות רציונליות מעל K.

להיפך, אם F שדה פונקציות רציונליות מעל K, אז (למשל) $\mathfrak{p}_\infty$ הוא מחלק בעל מעלה 1. ∎

הערה 16.3: כיוון שלשדה פונקציות רציונליות יש מחלק ראשוני בעל מעלה 1, מהשקילות במשפט 16.2 נובע, שיכולנו לכתוב במשפט "מחלק ראשוני" במקום "מחלק". ∎

תרגיל 16.4: *יהי F/K שדה פונקציות אלגבריות בעל גזע 0. הוכח שכל מחלק שלו ממעלה 0 הוא ראשי.*

17. שדות בעלי גזע 1

בפרק זה יהי F/K שדה פונקציות בעל גזע $g = 1$.

למה 17.1: *נניח כי* $F = K(x,y)$, *באשר* $y^2 = f(x)$ *ו־* $f \in K[X]$ *פולינום ממעלה* 3. *אז יש מחלק ראשוני* $\mathfrak{p}$ *ממעלה* 1 *כך ש־* $(x)_\infty = 2\mathfrak{p}$. *בפרט ל־* F/K *יש מחלק ראשוני ממעלה* 1.

הוכחה: בגלל $y^2 = f(x)$ ברור ש־$[F : K(x)] \le 2$. לא יתכן $F = K(x)$ כי אז F/K בעל גזע 0. לכן $[F : K(x)] = 2$. לפי משפט 8.8, $\deg(x)_\infty = 2$. מכאן שיש שלוש אפשרויות:

(א) $(x)_\infty = 2\mathfrak{p}$, באשר $\mathfrak{p}$ ראשוני ממעלה 1; או

(ב) $(x)_\infty = \mathfrak{p}$, באשר $\mathfrak{p}$ ראשוני ממעלה 2; או

(ג) $(x)_\infty = \mathfrak{p} + \mathfrak{q}$, באשר $\mathfrak{p}, \mathfrak{q}$ שני ראשוניים שונים ממעלה 1.

אבל $2(y)_\infty = (y^2)_\infty = \big(f(x)\big)_\infty = (\deg f)(x)_\infty = 3(x)_\infty$, לפי למה 15.1(ב). מכאן ברור שכל המקדמים של המחלק $(x)_\infty$ הם מספרים זוגיים. זה אומר שאפשרויות (ב), (ג) לא תיתכנה. לכן מתקיים (א). ∎

משפט "הפוך":

משפט 17.2: *יהי* F/K *שדה פונקציות בעל גזע* 1 *שיש לו מחלק ראשוני* $\mathfrak{p}$ *ממעלה* 1. *נניח כי* $\mathrm{char}\, K \ne 2$. *אז* $F = K(x,y)$, *באשר* $y^2 = f(x)$ *ו־* $f \in K[X]$ *פולינום ממעלה* 3 *ללא גורמים אי פריקים מרובים, ו־* $(x)_\infty = 2\mathfrak{p}$.

הוכחה: מתקיים $K = \mathcal{L}(0) \subseteq \mathcal{L}(\mathfrak{p}) \subseteq \mathcal{L}(2\mathfrak{p}) \subseteq \cdots$. יהי $n \in \mathbb{N}$. כיוון ש־$\deg n\mathfrak{p} = n > 0 = 2g - 2$, מתקיים $\dim \mathcal{L}(n\mathfrak{p}) = \deg n\mathfrak{p} + 1 - g = n$. לכן, אם נסמן $\mathcal{L}_0 = 0$ ו־$\mathcal{L}_n = \mathcal{L}(n\mathfrak{p})$ לכל $n \in \mathbb{N}$, אז $\dim \mathcal{L}_n = n$ לכל $n \ge 0$ ומתקיים $\mathcal{L}_0 = 0 \subset K = \mathcal{L}_1 \subset \mathcal{L}_2 \subset \mathcal{L}_3 \subset \cdots$.

לכן יש $x, y \in F$ כך ש־ $\mathcal{L}_1 = K = \mathrm{Sp}_K(1), \mathcal{L}_2 = \mathrm{Sp}_K(1,x), \mathcal{L}_3 = \mathrm{Sp}_K(1,x,y)$. כיוון ש־$x \in \mathcal{L}(2\mathfrak{p}) \smallsetminus \mathcal{L}(\mathfrak{p})$, לפי תרגיל 7.10 מתקיים $(x)_\infty = 2\mathfrak{p}$. באופן דומה $(y)_\infty = 3\mathfrak{p}$. לכן לפי משפט 8.8, $[F : K(x)] = \deg(x)_\infty = 2$.

אם $m, n \ge 0$ מספרים שלמים, אז $(x^m y^n)_\infty = (2m + 3n)\mathfrak{p}$. מכאן, לפי תרגיל 7.10,

$$1, x, x^2, x^3, y, xy, y^2 \in \mathcal{L}(6\mathfrak{p}) = \mathcal{L}_6. \tag{1}$$

ביתר דיוק, אם z אחד משבעת איברים במשוואה (1), אז $z \in \mathcal{L}_{k_z} \smallsetminus \mathcal{L}_{k_z - 1}$, באשר

$$k_z = \begin{cases} 1 & z = 1 \\ 2 & z = x \\ 3 & z = y \\ 4 & z = x^2 \\ 5 & z = xy \\ 6 & z = x^3 \\ 6 & z = y^2 \end{cases} \tag{2}$$

טענה: $1, x, y, x^2, xy, x^3$ בסיס של $\mathcal{L}_6$. אכן, $\dim \mathcal{L}_6 = 6$, בסדרה יש 6 איברים, ואף אחד מהם אינו צירוף לינארי של קודמיו, לפי (2) (כי קודמיו באיזה $\mathcal{L}_k$ והוא לא).

לפי הטענה y^2 הוא צירוף לינארי של יתר ששת האיברים ב־(1), כלומר, יש $a_1, \dots, a_6 \in K$ כך ש־

$$y^2 = a_1xy + a_2y + a_3x^3 + a_4x^2 + a_5x + a_6 \tag{3}$$

את (3) אפשר לרשום כך:

$$y^2 - (a_1x + a_2)y + \big(\frac{a_1x + a_2}{2}\big)^2 = a_3x^3 + a_4x^2 + a_5x + a_6 + \big(\frac{a_1x + a_2}{2}\big)^2,$$

(וכאן משתמשים בכך ש־$\mathrm{char}\ K \neq 2$) כלומר, אם נגדיר $y' = y - \frac{1}{2}(a_1x + a_2)$, אז

$$(y')^2 = f(x), \tag{4}$$

באשר $f \in K[X]$ ממעלה ≤ 3.

טענה: $F = K(x, y) = K(x, y')$. אכן, $v_\mathfrak{p}(x) = -2 < 0$, לכן אם $g(x) = \sum_{i=0}^n c_ix^i \in K[x]$ ממעלה $n \geq 0$ (ולכן $c_n \neq 0$) אז, לפי טענה 1.10(ג), $v_\mathfrak{p}\big(g(x)\big) = \min_{i:c_i\neq0} iv_\mathfrak{p}(x) = nv_\mathfrak{p}(x) = -2n$. לכן $v_\mathfrak{p}(g) \in 2\mathbb{Z}$ לכל $0 \neq g \in K[x]$ ולכן גם לכל $0 \neq g \in K(x)$. אבל $v_\mathfrak{p}(y) = -3$, לכן $y \notin K(x)$. כיוון ש־$[F : K(x)] = 2$, נקבל $F = K(x, y)$. ברור ש־$K(x, y) = K(x, y')$.

סיום ההוכחה: בלי הגבלת הכלליות f במשוואה (4) הוא מהמעלה המזערית האפשרית. אז אין ל־f גורמים אי פריקים מרובים. אכן, אם $q \in K[X]$ פולינום אי פריק ויש $g \in K[X]$ כך ש־$f = q^2g$, נגדיר $y'' = \frac{y'}{q(x)}$ ואז $F = K(x, y') = K(x, y'')$ ואילו $(y'')^2 = g(x)$ ו־$\deg g < \deg f$, בסתירה למזעריות $\deg f$.

לבסוף, כיוון ש־$g = 1$, לפי משפט 15.6 $\deg f = 3$. ∎

18. עקומים אליפטיים

יהי F/K שדה פונקציות בעל גזע 1 שיש לו מחלק ראשוני $\mathfrak{q}$ ממעלה 1. נניח כי $\operatorname{char} K \neq 2$. לפי משפט 17.2, אז $F = K(x,y)$, באשר $y^2 = f(x)$ ו־$f \in K[X]$ פולינום ממעלה 3 ללא שורשים מרובים. כמו כן $(x)_\infty = 2\mathfrak{q}$ ולכן $(y)_\infty = 3\mathfrak{q}$ (כי $2(y)_\infty = (y^2)_\infty = (f(x))_\infty = (\deg f)(x)_\infty = 3 \cdot 2\mathfrak{q}$).

למה 18.1: *יהיו $a, b \in K$ כך ש־$b^2 = f(a)$. אז*

$$R = K[x,y]_{(a,b)} = \left\{ \frac{g(x,y)}{h(x,y)} \middle| \, h, g \in K[X,Y],\ h(a,b) \neq 0 \right\}$$

חוג מקומי וקיים הומומורפיזם יחיד $\varphi\colon R \to K$ כך ש־$\varphi(x) = a, \varphi(y) = b$.

הוכחה:

טענה 1: $K[x,y] \cong K[x][Y]/(Y^2 - f(x))$. אכן, ההעתקה $Y \mapsto y$ משרה אפימורפיזם־K $K[x][Y] \to K[x][y] = K[x,y]$, לכן לפי משפט האיזומורפיזם הראשון די להראות שהגרעין שלו הוא האידאל $(Y^2 - f(x))$ של $K[x][Y]$. ברור ש־$Y^2 - f(x)$ הוא בגרעין ולכן $(Y^2 - f(x))$ הוא בגרעין. להיפך, אם $g(Y) \in K[x][Y]$ בגרעין, חילוק עם שארית נותן $q(Y) \in K[x][Y]$ ו־$g_0(x), g_1(x) \in K[x]$ כך שמתקיים

$$g(Y) = q(Y)(Y^2 - f(x)) + g_1(x)Y + g_0(x).$$

הצבת y במקום המשתנה Y נותנת $0 = g(y) = g_1(x)y + g_0(x)$. אבל $y \notin K(x)$, לכן $1, y$ בלתי תלויים לינארית מעל $K(x)$, ולכן $g_0(x) = g_1(x) = 0$. לכן $g(Y) = q(Y)(Y^2 - f(x)) \in (Y^2 - f(x))$.

טענה 2: *$x \mapsto a, y \mapsto b$ מגדירים הומומורפיזם־K $\varphi\colon K[x,y] \to K$.* אכן, ההצבה $x \mapsto a$ מגדירה הומומורפיזם $K[x] \to K$. הוא ניתן להרחבה להומומורפיזם $\varphi_1\colon K[x][Y] \to K[Y]$ על ידי $Y \mapsto Y$. ההצבה $Y \mapsto b$ מגדירה הומומורפיזם־K $K[Y] \to K$. ההרכבה $\varphi_2 \circ \varphi_1\colon K[x][Y] \to K$ מעתיקה את $(Y^2 - f(x))$ על 0, לכן, לפי משפט האיזומורפיזם הראשון, משרה הומומורפיזם־K $\varphi\colon K[x,y] \to K$ כך ש־$x \mapsto a, y \mapsto b$.

$$\begin{tikzcd}
K[x][Y] \arrow[r, "\varphi_1"] \arrow[dr] & K[Y] \arrow[r, "\varphi_2"] & K \\
& K[x][y] = K[x,y] \arrow[ur, "\varphi"] &
\end{tikzcd}$$

ברור ש־φ כזה הוא יחיד.

הגרעין של φ הוא $P = \{h(x,y) \mid h \in K[X,Y],\ h(a,b) = 0\}$. כיוון שהתמונה של φ הוא שדה, P הוא אידאל מרבי. לכן $R = \left\{ \frac{g(x,y)}{h(x,y)} \middle| \, h, g \in K[X,Y],\ h(a,b) \neq 0 \right\}$ הוא החוג המקומי, הלוקליזציה של $K[x,y]$ ב־P, וניתן להרחיב את φ באופן יחיד להומומורפיזם־K $R \to K$ (ראו הוכחה של משפט 3.1). ∎

למה 18.2: *בתנאים של הלמה הקודמת R הוא חוג הערכה של F. לכן קיים אתר יחיד $\varphi\colon F \to K \cup \infty$ כך ש־$\varphi(x) = a, \varphi(y) = b$.*

הוכחה: לפי למה 18.1 יש הומומורפיזם־K היחיד $\varphi\colon R \to K$ כך ש־$\varphi(x) = a, \varphi(y) = b$. לפי משפט 3.1 אפשר להרחיב את φ לאתר φ' של F. ויהי $\mathcal{O}$ חוג ההערכה של φ' ו־v הערכה מתאימה לו. אז $R \subseteq \mathcal{O}$. נראה כי $\mathcal{O} \subseteq R$. אז $R = \mathcal{O}$ ו־φ' יחיד, כי $\varphi'(F \smallsetminus \mathcal{O}) = \infty$. אכן, אם $z \in F \smallsetminus \mathcal{O}$, אז,לפי למה 1.14, $z^{-1} \in \mathcal{O} \smallsetminus \mathcal{O}^\times$ נמצא באידאל המרבי היחיד של $\mathcal{O}$, שהינו הגרעין של φ, ולכן $\varphi'(z) = \infty$.

נשים לב ש־$\gamma := v(x-a) > 0$. כיוון ש־$1, y-b$ הוא בסיס של F מעל $K(x)$, לכל $z \in F$ יש הצגה

$$z = \frac{g_0(x) + g_1(x)(y-b)}{h(x)}, \tag{1}$$

באשר $g_0, g_1, h \in K[X]$, $h \neq 0$, $\gcd(g_0, g_1, h) = 1$. נניח כי $z \in \mathcal{O}$, כלומר, $v(z) \geq 0$. יהי $k \geq 0$ המרבי כך ש־$(X-a)^k | h$, כלומר, $v\big(h(x)\big) = k\gamma$. נראה באינדוקציה על k ש־$z \in R$.

עבור $k = 0$ זה ברור. נניח $k \geq 1$. אז $v\big(h(x)\big) = k\gamma \geq \gamma$, לכן, כיוון ש־$v(z) \geq 0$,

$$v\big(g_0(x) + g_1(x)(y-b)\big) \geq \gamma. \tag{2}$$

כיוון ש־$v(y-b) > 0$, גם $v\big(g_1(x)(y-b)\big) > 0$. לפי (2), $v\big(g_0(x)\big) > 0$. מכאן ש־$(X-a) | g_0$, כלומר,

$$v\big(g_0(x)\big) \geq \gamma. \tag{3}$$

כיוון ש־$(y+b)(y-b) = f(x) - f(a)$, מתקיים

$$(y+b)z = \frac{(y+b)g_0(x) + \big(f(x)-f(a)\big)g_1(x)}{h(x)}.$$

המונה של אגף ימין הוא כפולה של $(x-a)$ ב־$K[x,y]$, לכן אפשר לצמצם ב־$(x-a)$. נשים לב ש־$y + b \in \mathcal{O}$, לכן $(y+b)z \in \mathcal{O}$. לפי הנחת האינדוקציה, $(y+b)z \in R$. אם $b \neq 0$ אז $\frac{1}{y+b} \in R$, לכן $z \in R$.

אם $b = 0$, אז a הוא שורש של f, לכן שורש פשוט. כלומר, $y^2 = (x-a)f_0(x)$, באשר $f_0 \in K[X]$, $f_0(a) \neq 0$. לכן $2v(y) = \gamma$ ומכאן $v(y) = \frac{1}{2}\gamma$. כעת, לפי (2) ו־(3), $v\big(g_1(x)y\big) \geq \gamma$, לכן $v\big(g_1(x)\big) \geq \gamma - \frac{1}{2}\gamma > 0$, ולכן $(X-a)|g_1$. לפי (3) גם $(X-a)|g_0$. זה בסתירה ל־$\gcd(g_0, g_1, h) = 1$.

∎

נגדיר

(א) $\mathbb{P}_1(K) = \{\mathfrak{p} \in \mathbb{P} |\ \deg \mathfrak{p} = 1\}$, אוסף המחלקים הראשוניים ממעלה 1 של F/K; $\mathbb{P}_1(K)$ הוא אוסף המחלקים הראשוניים ממעלה 1 של F/K;

(ב) $\mathbb{P}'_1(K) = \mathbb{P}_1(K) \smallsetminus \{\mathfrak{q}\}$;

(ג) $\mathcal{E}'(K) = \{(a,b) \in K^2 |\ b^2 = f(a)\}$.

מסקנה 18.3: *קיימת התאמה חד חד ערכית $\mathbb{P}'_1(K) \to \mathcal{E}'(K)$ הנתונה על ידי:* $\mathfrak{p} \mapsto (\varphi_\mathfrak{p}(x), \varphi_\mathfrak{p}(y))$.

הוכחה: נזכיר שאם $\mathfrak{p} \in \mathbb{P}_1(K)$, אז $\varphi_\mathfrak{p}\colon F \to K \cup \{\infty\}$ הוא האתר המתאים לו.

אמנם $\mathfrak{p}$ מסמן מחלקת שקילות של אתרי־K, אבל לפי תרגיל 1.21, שני אתרי־K $\varphi, \varphi'\colon F \to K \cup \{\infty\}$ הם שקולים אם ורק אם הם שווים.

יהי $\mathfrak{p} \in \mathbb{P}'_1(K)$. אז $\varphi_\mathfrak{p}(x) \neq \infty$. אכן, $\varphi_\mathfrak{p}(x) = \infty \Leftrightarrow v_\mathfrak{p}(x) < 0 \Leftrightarrow \mathfrak{p} \le (x)_\infty$, ו־$\mathfrak{q}$ (שהינו שונה מ־$\mathfrak{p}$) הוא המחלק הראשוני היחיד שמופיע ב־$(x)_\infty$. באופן דומה $\varphi_\mathfrak{p}(y) \neq \infty$.

אם $\varphi_\mathfrak{p}(x) = a, \varphi_\mathfrak{p}(y) = b$ אז $0 = \varphi_\mathfrak{p}\big(y^2 - f(x)\big) = b^2 - f(a)$.

לכן $\mathfrak{p} \mapsto (\varphi_\mathfrak{p}(x), \varphi_\mathfrak{p}(y))$ אכן מגדיר העתקה $\mathbb{P}'_1(K) \to \mathcal{E}'(K)$.

לפי למה 18.2 היא על וחד חד ערכית. ∎

נגדיר $\mathcal{E}(K) = \mathcal{E}'(K) \cup \{0\}$ ונרחיב את $\mathbb{P}'_1(K) \to \mathcal{E}'(K)$ להתאמה $\mathbb{P}_1(K) \to \mathcal{E}(K)$ על ידי $\mathfrak{q} \mapsto 0$.

תרגיל 18.4: *יהיו* $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathbb{P}_1(K)$. *אם* $[\mathfrak{p}_1] = [\mathfrak{p}_2]$ *(ז.א. המחלקות של $\mathfrak{p}_1, \mathfrak{p}_2$ שוות) אז* $\mathfrak{p}_1 = \mathfrak{p}_2$.

הוכחה: יש $z \in F^\times$ כך ש־$\mathfrak{p}_2 = (z) + \mathfrak{p}_1$. בפרט $(z) + \mathfrak{p}_1 \ge 0$, לכן $z \in \mathcal{L}(\mathfrak{p}_1)$. אבל $0 \le \mathfrak{p}_1$, לכן $K = \mathcal{L}(0) \subseteq \mathcal{L}(\mathfrak{p}_1)$, ו־$\deg \mathfrak{p}_1 = 1 > 0 = 2g - 2$, לכן $\dim \mathfrak{p}_1 = \deg \mathfrak{p}_1 + 1 - g = 1$, לכן $\mathcal{L}(\mathfrak{p}_1) = K$ ובפרט $z \in K^\times$. מכאן $(z) = 0$ ולכן $\mathfrak{p}_1 = \mathfrak{p}_2$. ∎

תהי $\mathcal{C}_0$ קבוצת מחלקות המחלקים של F/K שמעלתם 0. כלומר

$$\mathcal{C}_0 = \{\mathfrak{a} \in \mathcal{D} |\ \deg \mathfrak{a} = 0\}/\{(x) |\ x \in F^\times\}.$$

זוהי תת חבורה של חבורת מחלקות המחלקים של F/K.

למה 18.5: *ההעתקה* $\mathfrak{p} \mapsto [\mathfrak{p} - \mathfrak{q}]$ *היא התאמה חד חד ערכית* $\mathbb{P}_1(K) \to \mathcal{C}_0$.

הוכחה: אם $\deg \mathfrak{p} = 1$ אז $\deg(\mathfrak{p} - \mathfrak{q}) = 0$. לכן ההעתקה מוגדרת היטב.

נראה שהיא חד חד ערכית. נניח $[\mathfrak{p} - \mathfrak{q}] = [\mathfrak{p}' - \mathfrak{q}]$. אז $[\mathfrak{p}] = [\mathfrak{p}']$. לפי תרגיל 18.4, $\mathfrak{p} = \mathfrak{p}'$.

נראה שההעתקה היא על. יהי $\mathfrak{a} \in \mathcal{D}$ כך ש־$\deg \mathfrak{a} = 0$. אז $\deg(\mathfrak{a} + \mathfrak{q}) = 1 > 0 = 2g - 2$, לכן לפי משפט רימן־רוך $\dim(\mathfrak{a} + \mathfrak{q}) = 1 + 1 - g = 1$. לכן יש $z \in F^\times$ כך ש־$(z) + \mathfrak{q} + \mathfrak{a} \ge 0$. אבל $\deg\big((z) + \mathfrak{q} + \mathfrak{a}\big) = 1$, לכן קיים $\mathfrak{p}$ ראשוני כך ש־$\mathfrak{p} = (z) + \mathfrak{q} + \mathfrak{a}$. אז $[\mathfrak{p} - \mathfrak{q}] = [(z) + \mathfrak{a}] = [\mathfrak{a}]$. ∎

מסקנה 18.6: *קיימת התאמה חד חד ערכית בין $\mathcal{C}_0$ לבין $\mathcal{E}(K)$. התאמה זו הופכת את $\mathcal{E}(K)$ לחבורה אבלית. האפס שלה הוא הנקודה הנוספת 0.*

מהו כלל החיבור המפורש על $\mathcal{E}(K)$?

הערה 18.7: תהי $\mathfrak{p} \in \mathbb{P}'_1(K)$ ויהי $(a,b) \in \mathcal{E}'(K)$ המחלק הראשוני המתאים לה. תהי $\alpha X + \beta Y = \gamma$ משוואת ישר, $\alpha, \beta, \gamma \in K$, $\alpha \neq 0$ או $\beta \neq 0$. נסמן $z = \alpha x + \beta y - \gamma \in F$. אז (a,b) על ישר זה אם ורק אם $\varphi_{\mathfrak{p}}(z) = 0$.

אכן, $\varphi_{\mathfrak{p}}(z) = \alpha\varphi_{\mathfrak{p}}(x) + \beta\varphi_{\mathfrak{p}}(y) + \gamma = \alpha a + \beta b + \gamma$. ∎

הגדרה 18.8: נקודת האפס 0 נחשבת כנמצאת על ישר $\alpha X + \beta Y = \gamma$ אם $\beta = 0$. ∎

הערה 18.9: הסבר של הגדרה זו. רואים את $K \times K$ כחלק של המישורי הפרוייקטיבי $K^3 \smallsetminus \{0,0,0\}/\sim$ (באשר $(a,b,c) \sim (a',b',c')$ אם ורק אם יש $\lambda \in K^\times$ כך ש־$a' = \lambda a, b' = \lambda b, c' = \lambda c$): נקודה (a,b) של K^2 מזוהה עם המחלקה של $(a,b,1)$. אז העקום האליפטי שנתון על ידי $Y^2 = a_0 + a_1X + a_2X^2 + a_3X^3$ ב־K^2 הוא הצמצום של העקום במישור הפרוייקטיבי שנתון על ידי $(Y/Z)^2 = a_0 + a_1(X/Z) + a_2(X/Z)^2 + a_3(X/Z)^3$, כלומר, על ידי המשוואה ההומוגנית

$$Y^2Z = a_0Z^3 + a_1XZ^2 + a_2X^2Z + a_3X^3. \tag{4}$$

באופן דומה ישר שנתון על ידי $\alpha X + \beta Y = \gamma$ הוא חלק מהישר

$$\alpha X + \beta Y = \gamma Z \tag{5}$$

במישור הפרוייקטיבי.

המישור הפרוייקטיבי מכיל, מלבד K^2, את "הישר באינסוף" שמאופיין על ידי $Z = 0$. הוא מכיל נקודה יחידה של (4), היא מחלקת השקילות של $(0,1,0)$. (זאת הנקודה $0 \in \mathcal{E}(K)$.) היא נמצאת על (5) אם ורק אם $\beta = 0$.
∎

משפט 18.10: *תהיינה* $A_1, A_2, A_3 \in \mathcal{E}(K)$ *שונות. אז*

$$A_1 + A_2 + A_3 = 0 \tag{6}$$

(לפי החיבור שהוגדר לעיל) אם ורק אם A_1, A_2, A_3 *נמצאות על ישר אחד ב־* $\{0\} \cup (K \times K)$.

הוכחה: בלי הגבלת הכלליות $A_1, A_2 \neq 0$. לכל $1 \leq i \leq 3$ יהי $\mathfrak{p}_i \in \mathbb{P}_1(K)$ המחלק הראשוני המתאים ל־A_i (לכן $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathbb{P}'_1(K)$) ו־$\varphi_i$ האתר היחיד המתאים ל־$\mathfrak{p}_i$.

תהי $\alpha X + \beta Y = \gamma$ משוואת הישר דרך A_1, A_2. נסמן $z = \alpha x + \beta y - \gamma \in F$. כיוון ש־$(x)_\infty = 2\mathfrak{q}, (y)_\infty = 3\mathfrak{q}$, מתקיים $(z)_\infty = \begin{cases} 2\mathfrak{q} & \beta = 0 \\ 3\mathfrak{q} & \beta \neq 0 \end{cases}$.

(א) במקרה הראשון $\deg(z)_0 = \deg(z)_\infty = 2$. לפי הערה 18.7, $\varphi_1(z) = \varphi_2(z) = 0$, כלומר, $\mathfrak{p}_1, \mathfrak{p}_2 \leq (z)_0$. אילו A_3 היתה ב־$K \times K$ והיתה על הישר, אז היה $\mathfrak{p}_3 \leq (z)_0$, ולכן $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 \leq (z)_0$. בפרט $\deg(z)_0 \geq 3$, סתירה. מצד שני, 0 על הישר, לפי הגדרה 18.8. לכן A_3 על הישר אם ורק אם $A_3 = 0$.

לכן די להוכיח כי $A_1 + A_2 = 0$. כעת $\mathfrak{p}_1 + \mathfrak{p}_2 = (z)_0$, $2\mathfrak{q} = (z)_\infty$, לכן $\mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{q} = (z)$. מכאן $[\mathfrak{p}_1 - \mathfrak{q}] + [\mathfrak{p}_2 - \mathfrak{q}] = 0$, כלומר, $A_1 + A_2 = 0$.

(ב) במקרה השני 0 איננה על הישר. מתקיים $\deg(z)_0 = \deg(z)_\infty = 3$. אם $A_1 + A_2 + A_3 = 0$, אז

$$[\mathfrak{p}_1 - \mathfrak{q}] + [\mathfrak{p}_2 - \mathfrak{q}] + [\mathfrak{p}_3 - \mathfrak{q}] = 0 \,, \tag{7}$$

כלומר, יש $z' \in F^\times$ כך ש־

$$\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 - 3\mathfrak{q} = (z') . \tag{8}$$

כיוון ש־$\mathfrak{p}_1 + \mathfrak{p}_2 \le (z)_0$ ו־$\deg(z)_0 = 3$, יש $\mathfrak{p}_3' \in \mathbb{P}_1(K)$ כך ש־ $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3' = (z)_0$ ומכאן

$$\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3' - 3\mathfrak{q} = (z) . \tag{9}$$

כיוון ש־$(z)_0, (z)_\infty$ זרים, $\mathfrak{q} \neq \mathfrak{p}_3'$. מתוך (8) ו־(9) נובע $\mathfrak{p}_3 - \mathfrak{p}_3' = (z') - (z) = (z'/z)$, לכן $[\mathfrak{p}_3] = [\mathfrak{p}_3']$. לפי תרגיל 18.4, $\mathfrak{q} \neq \mathfrak{p}_3' = \mathfrak{p}_3$. אם כך, $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 = (z)_0$. בפרט $\varphi_3(z) = 0$, לכן A_3 על הישר.

להיפך, אם A_3 על הישר, אז, כאמור, $A_3 \neq 0$, ו־$\mathfrak{q} \neq \mathfrak{p}_3 \le (z)_0$. כיוון ש־$\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \le (z_0)$, ו־$\deg(z)_0 = 3$, מתקיים לכן $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 = (z)_0$. מכאן $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 - 3\mathfrak{q} = (z)$. מכאן (7) ולכן $A_1 + A_2 + A_3 = 0$. ∎

הערה 18.11: המשפט נכון גם אם A_1, A_2, A_3 אינן שונות, כאשר מבינים שנקודה A נמצאת בריבוי 2 על ישר, אם הוא עובר דרכה ומשיק בה לעקום. ∎

משפט 18.12 (משפט Mordell-Weil): *אם K שדה נוצר סופית אז $\mathcal{E}(K)$ חבורה נוצרת סופית.*

תרגיל 18.13: *הראה ש־$-(a,b) = (a,-b)$.*

תרגיל 18.14: *נניח כי $\mathrm{char}\ K \neq 2,3$. הראה שיש שינוי קואורדינטות*

$$x' = ax + b, \quad y' = cy + d, \qquad a, b \in K^\times,\ c, d \in K$$

שמעבירות את עקום $y^2 = f(x)$ לעקום בעל הצורה $y^2 = x^3 - g_2 x - g_3$, באשר $g_2, g_3 \in K$ כך ש־ $4g_2^3 - 27g_3^2 \neq 0$.

תרגיל 18.15: *נניח כי עקום אליפטי נתון על ידי $y^2 = x^3 - g_2 x - g_3$, באשר $g_2, g_3 \in K$ כך ש־$4g_2^3 - 27g_3^2 \neq 0$. תהיינה (a_i, b_i) על עקום, $i = 1,2,3$. אם*

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$$

ו־$(x_1, y_1) \neq (x_2, y_2)$ אז

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2$$

$$y_3 = \frac{y_1 - y_2}{x_1 - x_2} x_3 + \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2} .$$

19. הרחבות של שדות פונקציות

הגדרה 19.1: יהיו E/K, F/L שדות פונקציות (אלגבריות של משתנה אחד). נאמר ש־F/L **הרחבה של** E/K אם $E \subseteq F$, $K \subseteq L$, ו־$L \cap E = K$. ∎

$$\begin{tikzcd} E \arrow[r, dash] \arrow[d, dash] & F \arrow[d, dash] \\ K \arrow[r, dash] & L \end{tikzcd}$$

הגדרה 19.2: תהי F/L הרחבה של E/K.

יהי $\mathfrak{P}$ מחלק ראשוני של F/L ונניח שאתר $\varphi_{\mathfrak{P}}$ שמתאים לו אינו טריביאלי על E, כלומר, יש $0 \neq x \in E$ כך ש־$\varphi_{\mathfrak{P}}(x) = 0$. אז $\varphi_{\mathfrak{P}}|_E$ אתר של E/K. יהי $\mathfrak{p}$ המחלק שמתאים לו. נאמר ש־$\mathfrak{p}$ **מונח מתחת ל־$\mathfrak{P}$** ונסמן $\mathfrak{P}/\mathfrak{p}$.

תהי $v_{\mathfrak{P}}$ הערכה מנורמלת של F שמתאימה ל־$\mathfrak{P}$ כך ש־$v_{\mathfrak{P}}(F^\times) = \mathbb{Z}$. אז $v_{\mathfrak{P}}(E^\times) \leq v_{\mathfrak{P}}(F^\times)$, לכן $v_{\mathfrak{P}}(E^\times) = e\mathbb{Z}$, באשר $e \in \mathbb{N}$ (לא יתכן $e = 0$ כי $\varphi_{\mathfrak{P}}|_E$ אינו טריביאלי). נגדיר $v_{\mathfrak{p}}(x) = \frac{1}{e}v_{\mathfrak{P}}(x)$ לכל $x \in E$. אז $v_{\mathfrak{p}}$ הערכה על E ו־$v_{\mathfrak{p}}(E^\times) = \mathbb{Z}$. המספר e נקרא **אינדקס הסיעוף של** $\mathfrak{P}/\mathfrak{p}$ ויסומן $e(\mathfrak{P}/\mathfrak{p})$ או $e(\mathfrak{P})$ או $e_{F/E}(\mathfrak{P})$. לפי ההגדרה מתקיים

$$v_{\mathfrak{P}}(x) = e(\mathfrak{P}/\mathfrak{p})v_{\mathfrak{p}}(x), \qquad x \in E^\times.$$

יהיו

- $\mathcal{O}_{\mathfrak{P}}$ חוג ההערכה של $\mathfrak{P}$ ב־F ויהיו $M_{\mathfrak{P}}$ האידאל המרבי שלו,
- $\mathcal{O}_{\mathfrak{p}}$ חוג ההערכה של $\mathfrak{p}$ ב־E ויהי $M_{\mathfrak{p}}$ האידאל המרבי שלו.

$$(1) \qquad \begin{tikzcd} E \arrow[r, dash] \arrow[d, dash] & F \arrow[d, dash] \\ K \arrow[r, dash] & L \end{tikzcd} \qquad \begin{tikzcd} L \arrow[r] & \mathcal{O}_{\mathfrak{P}} \arrow[r] & \mathcal{O}_{\mathfrak{P}}/M_{\mathfrak{P}} = F_{\mathfrak{P}} \\ K \arrow[r] \arrow[u] & \mathcal{O}_{\mathfrak{p}} \arrow[r] \arrow[u] & \mathcal{O}_{\mathfrak{p}}/M_{\mathfrak{p}} = E_{\mathfrak{p}} \arrow[u, dashed] \end{tikzcd} \qquad \begin{tikzcd} E_{\mathfrak{p}} \arrow[r, dash] \arrow[d, dash] & F_{\mathfrak{P}} \arrow[d, dash] \\ K \arrow[r, dash] & L \end{tikzcd}$$

אז $\mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{P}}$, $M_{\mathfrak{p}} \subseteq M_{\mathfrak{P}}$, כי $\varphi_{\mathfrak{P}}$ הרחבה של $\varphi_{\mathfrak{p}}$. כמו כן $\mathcal{O}_{\mathfrak{p}} = E \cap \mathcal{O}_{\mathfrak{P}}$, $M_{\mathfrak{p}} = E \cap M_{\mathfrak{P}}$, וקיים התרשים השמאלי לעיל של הכלות של שדות. המעלה $[F_{\mathfrak{P}} : E_{\mathfrak{p}}]$ נקראת **מעלת שדות השאריות של $\mathfrak{P}$ מעל** $\mathfrak{p}$ ותסומן $f(\mathfrak{P}/\mathfrak{p})$. לפי תרשים השמאלי ב־$(1)$,

$$[L:K]\deg\mathfrak{P} = f(\mathfrak{P}/\mathfrak{p})\deg\mathfrak{p} \qquad (2)$$

(כאשר חלק מהביטויים יכולים להיות ∞). ∎

למה 19.3: *יהי $\mathfrak{p}$ מונח מתחת ל-$\mathfrak{P}$. אז שלוש הטענות הבאות שקולות:*

(א) L/K *סופית*

(ב) F/E *סופית*

(ג) $F_{\mathfrak{P}}/E_{\mathfrak{p}}$ *סופית (כלומר, $f(\mathfrak{P}/\mathfrak{p}) < \infty$).*

השקילות נשארת (בלי הביטוי בסוגריים), אם במקום "סופית" נכתוב "אלגברית" בכל מקום.

הוכחה: (א) $\Leftrightarrow$ (ב): יהי $x \in E \smallsetminus K$. אז $x \in F \smallsetminus L$ (אם $x \in L$ אז $x \in E \cap L = K$, סתירה). לכן x טרנסצנדנטי מעל K, L. מכאן $[L : K] = [L(x) : K(x)]$ (בסיס של L מעל K הוא בסיס של $L(x)$ מעל $K(x)$). כמו כן $[E : K(x)], [F : L(x)] < \infty$. לכן השקילות נובעת לפי נוסחת מכפלת המעלות של ההרחבות שבמלבן העליון של התרשים הבא.

$$\begin{tikzcd}
E \arrow[r, dash] \arrow[d, dash] & F \arrow[d, dash] \\
K(x) \arrow[r, dash] \arrow[d, dash] & L(x) \arrow[d, dash] \\
K \arrow[r, dash] & L
\end{tikzcd}$$

(א) $\Leftrightarrow$ (ג): לפי (2).

באופן דומה לגבי האלגבריות במקום הסופיות. ∎

תרגיל 19.4: *תהי F/E הרחבה אלגברית של שדות ויהי φ אתר לא טריביאלי של F. הוכח כי $\varphi|_E$ הוא אתר לא טריביאלי של E.*

הוכחה: נוכיח שאם $\varphi|_E$ הוא אתר טריביאלי של E, אז φ אתר טריביאלי של F.

בלי הגבלת הכלליות F/E סופית. אכן, יהי $x \in F$. אז $E(x)$ הרחבה סופית של E. אם נראה ש-$\varphi|_{E(x)}$ טריביאלי, אז $\varphi(x) \neq \infty$. זה נכון לכל $x \in F$ ולכן φ טריביאלי.

תהי v הערכה מתאימה ל-φ. אז $v(F^\times)$ חבורת הערכה ו-$0 = v(E^\times) \le v(F^\times)$. לפי מסקנה 4.3, $\left(v(F^\times) : v(E^\times)\right) < \infty$, לכן $v(F^\times)$ סופית. לפי מסקנה 1.5, $v(F^\times) = 0$. לכן φ טריביאילי. ∎

תרגיל 19.5: *תהי F/L הרחבה של E/K ו-F'/L' הרחבה של F/L. יהי $\mathfrak{p}$ מחלק ראשוני של E/K, יהי $\mathfrak{P}$ מחלק ראשוני של F/L שמונח מעליו ו-$\mathfrak{P}'$ מחלק ראשוני של F'/L' שמונח מעליו. אז*

$$e(\mathfrak{P}'/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{P})e(\mathfrak{P}/\mathfrak{p}), \qquad f(\mathfrak{P}'/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{P})f(\mathfrak{P}/\mathfrak{p}).$$

$$\begin{array}{ccc} \mathfrak{P}' & \qquad & F' \\ | & & | \\ \mathfrak{P} & & F \\ | & & | \\ \mathfrak{p} & & E \end{array}$$

אם F/L הרחבה של E/K ו־$x \in E$ אז ל־(x) יש שתי משמעויות שונות: מחלק ראשי של F/L ומחלק ראשי של E/K. כדי להבדיל ביניהן, נשתמש בסימון $(x)_E, (x)_F$, בהתאמה. באופן דומה $(x)_{E,\infty}, (x)_{F,\infty}$ עבור מחלק הקטבים ו־ $(x)_{E,0}, (x)_{F,0}$ עבור מחלק האפסים.

תרגיל 19.6: *יהי E/K שדה פונקציות אלגבריות ויהי $\mathfrak{p}$ מחלק ראשוני של E/K. אז קיים $x \in E \smallsetminus K$ כך ש־ $(x)_{E,\infty} = k\mathfrak{p}$, עבור איזה $k \in \mathbb{N}$.*

הוכחה: יהי g הגזע של E/K. נבחר $n \in \mathbb{N}$ גדול מספיק. אז לפי משפט רימן־רוך

$$\dim n\mathfrak{p} = \deg n\mathfrak{p} + 1 - g \geq n + 1 - g \geq 2 \,.$$

לכן יש $x \in E \smallsetminus K$ כך ש־$(x)_E + n\mathfrak{p} \geq 0$. מכאן $(x)_{E,\infty} = k\mathfrak{p}$, באשר $0 \leq k \leq n$. אבל $x \notin K$, לכן $(x)_{E,\infty} \neq 0$, ולכן $1 \leq k$. ∎

למה 19.7: *תהי F/L הרחבה של E/K ויהי $\mathfrak{p}$ מחלק ראשוני של E/K. אז קבוצת המחלקים הראשוניים של F/L שמונחים מעל $\mathfrak{p}$ היא סופית ולא ריקה.*

הוכחה: לפי תרגיל 19.6 קיים $x \in E \smallsetminus K$ כך ש־$(x)_{E,\infty} = k\mathfrak{p}$, עבור איזה $k \in \mathbb{N}$.

אבל גם $x \in F^\times$, לכן אפשר לכתוב

$$(x)_{F,\infty} = \sum_{i=1}^{r} m_i \mathfrak{P}_i \tag{3}$$

באשר $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ הם מחלקים ראשוניים שונים של F/L ו־$m_i \in \mathbb{N}$ לכל i. כיוון ש־$x \notin L$ (אחרת $x \in E \cap L = K$, סתירה), $r \geq 1$. לכן די להוכיח:

טענה: *מחלק ראשוני $\mathfrak{P}$ של F/L מונח מעל $\mathfrak{p}$ אם ורק אם $\mathfrak{P} \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$.*

נוכיח את הטענה:

אם $\mathfrak{P}$ מונח מעל $\mathfrak{p}$ אז $v_{\mathfrak{P}}(x) < 0$, כי $v_{\mathfrak{p}}(x) < 0$, ולכן $\mathfrak{P} \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$, לפי הגדרת $(x)_{F,\infty}$.

להיפך, יהי $\mathfrak{P} = \mathfrak{P}_i$. אז $v_{\mathfrak{P}}(x) < 0$. לכן מתחת ל־$\mathfrak{P}$ מונח מחלק ראשוני $\mathfrak{q}$ של E/K (הצמצום של אתר מתאים ל־$\mathfrak{P}$ ל־E אינו טריביאלי, כי הוא מעתיק את $x \in E$ ל־∞) שמקיים $v_{\mathfrak{q}}(x) < 0$. לכן $k\mathfrak{p} = (x)_{E,\infty} \geq \mathfrak{q}$, ומכאן $\mathfrak{q} = \mathfrak{p}$. ∎

משפט 19.8 (השוויון היסודי): *תהי F/L הרחבה סופית של E/K. יהי $\mathfrak{p}$ מחלק ראשוני של E/K. אז*

$$[F:E]=\sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}).$$

הוכחה: יהיו $\mathfrak{P}_1,\dots,\mathfrak{P}_r$ המחלקים הראשוניים השונים של F/L המונחים מעל $\mathfrak{p}$. לפי תרגיל 19.6 קיים $x\in E\smallsetminus K$ כך ש־$(x)_{E,\infty}=k\mathfrak{p}$, עבור איזה $k\in\mathbb{N}$. לפי הטענה בהוכחה של למה 19.7 מתקיים (3) $(x)_{F,\infty}=\sum_{i=1}^r m_i\mathfrak{P}_i$. אז

$$[E:K(x)]=\deg(x)_{E,\infty}=k\deg\mathfrak{p}. \tag{4}$$

כמו כן, $m_i=-v_{\mathfrak{P}_i}(x)=e(\mathfrak{P}_i/\mathfrak{p})\big(-v_{\mathfrak{p}}(x)\big)=e(\mathfrak{P}_i/\mathfrak{p})k$ ולכן

$$[F:L(x)]=\deg(x)_{F,\infty}=\sum_{i=1}^r m_i\deg\mathfrak{P}_i=k\sum_{i=1}^r e(\mathfrak{P}_i/\mathfrak{p})\deg\mathfrak{P}_i.$$

נכפיל משוואה זו ב־$[L(x):K(x)]=[L:K]$ ונקבל, לפי (2)

$$[F:K(x)]=k\sum_{i=1}^r e(\mathfrak{P}_i/\mathfrak{p})[L:K]\deg\mathfrak{P}_i=k\deg\mathfrak{p}\sum_{i=1}^r e(\mathfrak{P}_i/\mathfrak{p})f(\mathfrak{P}_i/\mathfrak{p}).$$

נחלק משוואה זו במשוואה (4) ונקבל את השוויון המבוקש. ∎

מסקנה 19.9: *בתנאים של המשפט,* $\#\{\mathfrak{P}|\ \mathfrak{P}/\mathfrak{p}\}, e(\mathfrak{P}/\mathfrak{p}), f(\mathfrak{P}/\mathfrak{p})\le[F:E]$.

20. הרחבות נורמליות

יהיו $F/L, F'/L'$ שדות פונקציות נניח שיש איזומורפיזם שדות $\sigma\colon F \to F'$ כך ש־$\sigma(L) = L'$.

לכל הערכה v של F מתאימה הערכה (תסומן σv) של F' המוגדרת על ידי $(\sigma v)(\sigma x) = v(x)$ לכל $x \in F$. במלים אחרות, $\mathcal{O}_{\sigma v} = \sigma(\mathcal{O}_v)$ (ו־$M_{\sigma v} = \sigma(M_v)$). באופן כזה σ משרה התאמה בין ההערכות על F לבין ההערכות על $F' = \sigma(F)$.

הערכות שקולות עוברות להערכות שקולות, הערכות טריביאליות על L עוברות להערכות טריביאליות על L', לכן σ משרה התאמה חד חד ערכית $\mathfrak{P} \mapsto \sigma\mathfrak{P}$ בין המחלקים הראשוניים של F/L לבין המחלקים הראשוניים של F'/L'. כמו כן σ משרה איזומורפיזם של שדות השאריות $\bar{\sigma}\colon F_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}/M_{\mathfrak{P}} \to F'_{\mathfrak{P}'} = \mathcal{O}_{\sigma\mathfrak{P}}/M_{\sigma\mathfrak{P}}$

$$\begin{tikzcd} y \arrow[d, mapsto, "\pi_{\mathfrak{P}}"] \\ \pi_{\mathfrak{P}}(y) \end{tikzcd} \qquad \begin{tikzcd} \mathcal{O}_{\mathfrak{P}} \arrow[r, "\sigma"] \arrow[d, "\pi_{\mathfrak{P}}"] & \mathcal{O}_{\mathfrak{P}'} \arrow[d, "\pi_{\mathfrak{P}'}"] \\ F_{\mathfrak{P}} \arrow[r, "\bar{\sigma}"] & F_{\mathfrak{P}'} \end{tikzcd} \qquad \begin{tikzcd} y' \arrow[d, mapsto, "\pi_{\mathfrak{P}'}"] \\ \pi_{\mathfrak{P}'}(y') \end{tikzcd} \qquad \bar{\sigma}\big(\pi_{\mathfrak{P}}(y)\big) = \pi_{\mathfrak{P}'}\big(\sigma(y)\big)$$

לפי משפט האיזומורפיזם הראשון. בפרט, $\deg \mathfrak{P} = \deg \sigma\mathfrak{P}$.

הגדרה 20.1: הרחבה F/L של שדה פונקציות E/K נקראת **נורמלית** אם F/E הרחבה (אלגברית) נורמלית.

טענה 20.2: *אם F/L הרחבה נורמלית של E/K אז L/K נורמלית.*

הוכחה: כיוון ש־F/E אלגברית, גם L/K אלגברית (למה 19.3). יהי $f \in K[X]$ אי פריק בעל שורש ב־L. צריך להראות שכל שורשיו ב־L.

לפי תרגיל 6.7, f אי פריק מעל E. יש לו שורש ב־F, כי $L \subseteq F$. בגלל הנורמליות כל שורשיו ב־F. אבל הם אלגבריים מעל L לכן הם ב־$\tilde{L} \cap F = L$. ∎

יהי σ אוטומורפיזם של F מעל E. בפרט $\sigma|_K = \mathrm{id}$, לכן לפי טענה 20.2, $\sigma(L) = L$. אם מחלק ראשוני $\mathfrak{P}$ של F/L מונח מעל מחלק ראשוני $\mathfrak{p}$ של E/K, אז

$$e(\sigma\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}), \qquad f(\sigma\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}). \tag{1}$$

(זהו מקרה פרטי של הדיון לעיל, עם $F' = F$ ו־$L' = L$).

הערה 20.3: נזכור שלכל הרחבת שדות סופית F/E יש שדה ביניים E_s, ההרחבה הפרידה הגדולה ביותר של E בתוך F. ההרחבה F/E_s הינה אי פרידה טהורה. לכן

$$q := [F : E]_i := [F : E_s] = \begin{cases} 1 & \mathrm{char}\ E = 0 \\ p \text{ חזקה של} & \mathrm{char}\ E = p > 0 \end{cases}.$$

לכל $x \in F$ מתקיים $x^q \in E_s$ ולכן כל שיכון $\sigma\colon E_s \to M$ לתוך שדה סגור אלגברית M ניתן להרחבה באופן יחיד לשיכון $\sigma\colon F \to M$.

אם F/E נורמלית, אז E_s/E הרחבת גלואה. במקרה זה אפשר לזהות את $G := \mathrm{Aut}(F/E)$ עם $\mathrm{Gal}(E_s/E)$. זוהי חבורה סופית. אם $z \in E_s$ אז $\prod_{\sigma\in G}\sigma z \in E_s$ נשמר על ידי כל אברי G, לכן הוא איבר של E. לכן לכל $x \in F$ מתקיים $N_{F/E}(x) := (\prod_{\sigma\in G}\sigma x)^q = \prod_{\sigma\in G}\sigma(x^q) \in E$. ■

מעתה תהי F/L הרחבה נורמלית סופית של E/K. נגדיר G, q, E_s כמו בהערה 20.3.

יהי $\mathfrak{p}$ מחלק ראשוני של E/K ויהי $\mathfrak{P}$ מחלק ראשוני של F/L מונח מעליו.

משפט 20.4: *יהיו $\mathfrak{P}, \mathfrak{P}'$ שני מחלקים ראשוניים של F/L המונחים מעל $\mathfrak{p}$. אז יש אוטומורפיזם σ של F מעל E כך ש- $\sigma\mathfrak{P} = \mathfrak{P}'$.*

הוכחה: נניח בשלילה כי $\sigma\mathfrak{P} \neq \mathfrak{P}'$ לכל $\sigma \in G$. אז הקבוצות $\{\sigma\mathfrak{P}|\ \sigma \in G\}$, $\{\sigma\mathfrak{P}'|\ \sigma \in G\}$ זרות זו לזו, כי אם כך ש-$\tau\mathfrak{P} = \sigma\mathfrak{P}'$, אז $\mathfrak{P}' = \sigma^{-1}\tau\mathfrak{P}$, סתירה. לפי משפט הקירוב החלש יש $x \in F$ כך ש- $v_{\sigma\mathfrak{P}}(x) > 0$, $v_{\sigma\mathfrak{P}'}(x) < 0$ לכל $\sigma \in G$.

יהי $y = N_{F/E}(x) = (\prod_{\sigma\in G}\sigma x)^q \in E$. אז

$$v_{\mathfrak{P}}(y) = q\sum_{\sigma\in G} v_{\mathfrak{P}}(\sigma x) = q\sum_{\sigma\in G} v_{\sigma^{-1}\mathfrak{P}}(x) > 0,$$

לכן $v_{\mathfrak{p}}(y) = \frac{1}{e(\mathfrak{P}/\mathfrak{p})}v_{\mathfrak{P}}(y) > 0$. באופן דומה $v_{\mathfrak{P}'}(y) < 0$, לכן $v_{\mathfrak{p}}(y) < 0$. סתירה. ■

הגדרה 20.5: התת חבורה $D(\mathfrak{P}) = D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G|\ \sigma\mathfrak{P} = \mathfrak{P}\}$ של G נקראת **חבורת הפירוק של** $\mathfrak{P}$. ■

מסקנה 20.6: *מעל $\mathfrak{p}$ מונחים בדיוק $\big(G : D(\mathfrak{P})\big)$ מחלקים ראשוניים של F/L.*

משפט 20.7: *(א) הרחבת שדות השאריות $F_{\mathfrak{P}}/E_{\mathfrak{p}}$ היא נורמלית סופית.*

(ב) *ההעתקה $\bar\sigma \mapsto \sigma$ היא אפימורפיזם חבורות $D(\mathfrak{P}) \to \mathrm{Aut}(F_{\mathfrak{P}}/E_{\mathfrak{p}})$. הוא נתון על ידי*

$$\bar\sigma\bar y = \overline{\sigma y}, \qquad \text{לכל } y \in \mathcal{O}_{\mathfrak{P}}, \tag{2}$$

באשר $\bar y \mapsto y$ היא העתקת המנה $\mathcal{O}_{\mathfrak{P}} \to F_{\mathfrak{P}}$ מודולו האידאל המרבי של $\mathcal{O}_{\mathfrak{P}}$.

$$\begin{tikzcd}
F \supseteq \mathcal{O}_{\mathfrak{P}} \arrow[r] \arrow[d, dash] & F_{\mathfrak{P}} \arrow[d, dash] \\
E \supseteq \mathcal{O}_{\mathfrak{p}} \arrow[r] & E_{\mathfrak{p}}
\end{tikzcd}$$

הוכחה: ההרחבה סופית לפי למה 19.3. נראה שהיא נורמלית. יהי $\bar y \in F_{\mathfrak{P}}$. נראה שכל הצמודים שלו מעל $E_{\mathfrak{p}}$ נמצאים בתוך $F_{\mathfrak{P}}$.

טענה: *ל־$\bar{y}$ יש מייצג* $y \in \mathcal{O}_\mathfrak{P}$ *כך ש־*$v_\mathfrak{P}(\sigma y) \geq 0$ *לכל* $\sigma \in G$ *ואפילו* $v_\mathfrak{P}(\sigma y) > 0$ *לכל* $\sigma \in G \setminus D(\mathfrak{P})$.

אכן, יש $y' \in \mathcal{O}_\mathfrak{P}$ כך ש־$\overline{y'} = \bar{y}$. בפרט $v_\mathfrak{P}(y') \geq 0$. נשים לב שאם $\sigma \in G \setminus D(\mathfrak{P})$ אז $\sigma\mathfrak{P} \neq \mathfrak{P}$, ולכן $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$. לכן לפי משפט הקירוב החלש יש $y \in F$ כך ש־

$$v_\mathfrak{P}(y - y') > 0,$$

$$v_\mathfrak{P}(\sigma y) = v_{\sigma^{-1}\mathfrak{P}}(y) > 0, \qquad \text{לכל } \sigma \in G \setminus D(\mathfrak{P}).$$

כיוון ש־$v_\mathfrak{P}(y') \geq 0$ ו־$v_\mathfrak{P}(y - y') \geq 0$, מתקיים $v_\mathfrak{P}(y) \geq 0$. אם $\sigma \in D(\mathfrak{P})$, אז $\sigma\mathfrak{P} = \mathfrak{P}$, ולכן $\sigma^{-1}\mathfrak{P} = \mathfrak{P}$, ומכאן $v_\mathfrak{P}(\sigma y) = v_{\sigma^{-1}\mathfrak{P}}(y) = v_\mathfrak{P}(y) \geq 0$ לכל $\sigma \in D(\mathfrak{P})$. בכך הוכחה הטענה.

יהי

$$f(X) = \prod_{\sigma \in G} (X - \sigma y)^q = \prod_{\sigma \in G} \big(X^q - \sigma(y^q)\big).$$

אז $f(X) \in \mathcal{O}_\mathfrak{P}[X]$. אבל $y^q \in E_s$, לכן $f \in E_s[X]$ והמקדמים שלו נשמרים על ידי אברי G, ולכן הם ב־E ובפרט ב־$E \cap \mathcal{O}_\mathfrak{P} = \mathcal{O}_\mathfrak{p}$. תהי $\bar{f}(X)$ הרדוקציה של $f(X)$ מודולו האידאל המרבי של $\mathcal{O}_\mathfrak{P}$. לפי הטענה

$$\bar{f}(X) = \prod_{\sigma \in G} (X - \overline{\sigma y})^q = \prod_{\sigma \in D(\mathfrak{P})} (X - \overline{\sigma y})^q X^{|G \setminus D(\mathfrak{P})|} \in E_\mathfrak{p}[X],$$

כי $v_\mathfrak{P}(\sigma y) > 0$, ולכן $\overline{\sigma y} = 0$, לכל $\sigma \in G \setminus D(\mathfrak{P})$. בפרט

$$g(X) := \prod_{\sigma \in D(\mathfrak{P})} (X - \overline{\sigma y})^q \in E_\mathfrak{p}[X]. \tag{3}$$

נשים לב שכל שורשיו ב־$F_\mathfrak{P}$. כיוון ש־$\bar{y}$ שורשו, כל הצמודים של $\bar{y}$ מעל $E_\mathfrak{p}$ הם שורשיו, ולכן ב־$F_\mathfrak{P}$. לכן $F_\mathfrak{P}/E_\mathfrak{p}$ נורמלית.

(ב) אם $\sigma \in D(\mathfrak{P})$, אז $\sigma\mathfrak{P} = \mathfrak{P}$, לכן לפי הדיון בתחילת הפרק $\sigma\colon \mathcal{O}_\mathfrak{P} \to \mathcal{O}_\mathfrak{P}$ משרה $\bar{\sigma}\colon F_\mathfrak{P} \to F_\mathfrak{P}$.
אם $\sigma, \tau \in D(\mathfrak{P})$ אז $(\bar{\sigma}\bar{\tau})\bar{y} = \bar{\sigma}(\bar{\tau}\bar{y}) = \bar{\sigma}\overline{\tau y} = \overline{\sigma(\tau y)} = \overline{\sigma\tau y} = \overline{\sigma\tau}\bar{y}$ לכל $y \in \mathcal{O}_\mathfrak{P}$, לכן $\overline{\sigma\tau} = \bar{\sigma}\bar{\tau}$. לכן $\sigma \mapsto \bar{\sigma}$ הומומורפיזם.

נראה שהוא על. תהי $\tau \in \mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})$. יהי N שדה השבת של $\mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})$. אז $N/E_\mathfrak{p}$ הרחבה אי פרידה טהורה ו־$F_\mathfrak{P}/N$ הרחבת גלואה סופית, בפרט פרידה, לכן יש לה איבר פרימיטיבי $\bar{y} \in F_\mathfrak{P}$. לפי ההוכחה של (א) $\bar{y}$ הוא שורש של $g(X)$ ממשוואה (3). אז גם $\tau\bar{y}$ שורש שלו, לכן יש $\sigma \in D(\mathfrak{P})$ כך ש־$\tau\bar{y} = \overline{\sigma y} = \bar{\sigma}\bar{y}$. בנוסף לכך הצמצומים של $\bar{\sigma}, \tau$ ל־N הם הזהות, ובפרט שווים. לכן $\bar{\sigma} = \tau$. ∎

הגדרה 20.8: $I(\mathfrak{P}/\mathfrak{p}) := \mathrm{Ker}\,\big(D(\mathfrak{P}) \to \mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})\big)$ תיקרא **חבורת ההתמדה** של $\mathfrak{P}$ מעל $\mathfrak{p}$. ∎

מסקנה 20.9: $|D(\mathfrak{P})| = |I(\mathfrak{P})| \cdot |\mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})|$.

תרגיל 20.10: *יהי* $\tau \in G$. *אז* $D(\tau\mathfrak{P}) = \tau D(\mathfrak{P})\tau^{-1}$, $I(\tau\mathfrak{P}) = \tau I(\mathfrak{P})\tau^{-1}$.

מסקנה 20.11: *נסמן* $e = e(\mathfrak{P}/\mathfrak{p}), f = f(\mathfrak{P}/\mathfrak{p})$.

(א) $e(\sigma\mathfrak{P}/\mathfrak{p}) = e$, $f(\sigma\mathfrak{P}/\mathfrak{p}) = f$, *לכל* $\sigma \in G$.

(ב) $[F : E] = efr$, *באשר* r *מספר המחלקים הראשוניים של* F *שמונחים מעל* $\mathfrak{p}$.

(ג) $e = \frac{[F:E]_i}{[F_\mathfrak{P}:E_\mathfrak{p}]_i} \cdot |I(\mathfrak{P}/\mathfrak{p})|$

(ד) $ef = [F : E]_i \cdot |D(\mathfrak{P}/\mathfrak{p})|$

הוכחה: (א) ראה (1).

(ב) לפי משפט 20.4, כל המחלקים הראשוניים מעל $\mathfrak{p}$ הם מהצורה $\sigma\mathfrak{P}$, באשר $\sigma \in G$. לפי (א) לכולם אינדקס סיעוף e ומעלת השאריות f. לכן הנוסחה נובעת מהשוויון היסודי (משפט 19.8).

(ג) לפי (ב), $e = \frac{[F:E]}{fr}$. כעת,

$$[F : E] = [F : E_s] \cdot [E_s : E] = [F : E]_i \cdot |G| \tag{4}$$

$$f = [F_\mathfrak{P} : E_\mathfrak{p}] = [F_\mathfrak{P} : E_\mathfrak{p}]_i \cdot |\mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})|, \tag{5}$$

ולפי מסקנה 20.6 ומסקנה 20.9,

$$|G| = r|D(\mathfrak{P})| = r \cdot |I(\mathfrak{P})| \cdot |\mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})|. \tag{6}$$

אם נציב זאת בנוסחה הראשונה, נקבל את המסקנה: נסמן $A = \mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})$, אז

$$e = \frac{[F:E]}{fr} = \frac{[F:E]_i \cdot |G|}{[F_\mathfrak{P}:E_\mathfrak{p}]_i \cdot |A| r} = \frac{[F:E]_i \cdot r \cdot |I(\mathfrak{P})| \cdot |A|}{[F_\mathfrak{P}:E_\mathfrak{p}]_i \cdot |A| r} = \frac{[F:E]_i}{[F_\mathfrak{P}:E_\mathfrak{p}]_i} \cdot |I(\mathfrak{P})|.$$

(ד) מהשוויון היסודי נובע $ef = \frac{[F:E]}{r}$. נציב את (4) ו־(6) בנוסחה זו כדי לקבל את המבוקש:

$$ef = \frac{[F:E]}{r} = \frac{[F:E]_i \cdot |G|}{r} = \frac{[F:E]_i \cdot r|D(\mathfrak{P})|}{r} = [F:E]_i \cdot |D(\mathfrak{P})|. \qquad \blacksquare$$

תרגיל 20.12: *נניח כי* F/E *נורמלית. הוכח*

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Aut}(F/E) \mid v_\mathfrak{P}(\sigma z - z) \geq 0 \text{ לכל } z \in \mathcal{O}_\mathfrak{P}\},$$

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Aut}(F/E) \mid v_\mathfrak{P}(\sigma z - z) > 0 \text{ לכל } z \in \mathcal{O}_\mathfrak{P}\}.$$

תרגיל 20.13: *בהנחות של הפרק תהי* F'/L' *הרחבה של* E/K, *כך ש־*F/L *(הרחבת נורמלית של* E/K*) היא הרחבה של* F'/L'. *יהי* $\mathfrak{P}' = \mathfrak{P} \cap F'$ *מחלק ראשוני של* F'/L' *מתחת ל־*$\mathfrak{P}$ *ומעל* $\mathfrak{p}$. *יהיו* $E_\mathfrak{p} \subseteq F'_{\mathfrak{P}'} \subseteq F_\mathfrak{P}$ *שדות השאריות. יהי* $\sigma \mapsto \bar{\sigma}$ *האפימורפיזם* $D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})$ *של משפט 20.7(ב).*

$$\begin{array}{ccccc} E & \text{———} & F' & \text{———} & F \\ \mathfrak{p} & & \mathfrak{P}' & & \mathfrak{P} \\ E_\mathfrak{p} & \text{———} & F'_{\mathfrak{P}'} & \text{———} & F_\mathfrak{P} \end{array}$$

הוכיחו

(א) *יהיו* $\sigma, \tau \in D(\mathfrak{P}/\mathfrak{p}) \leq \mathrm{Aut}(F/E)$. *אז*

$$\sigma|_{F'} = \tau|_{F'} \quad \Leftrightarrow \quad \sigma D(\mathfrak{P}/\mathfrak{P}') = \tau D(\mathfrak{P}/\mathfrak{P}').$$

$$\bar{\sigma}|_{F'_{\mathfrak{P}'}} = \bar{\tau}|_{F'_{\mathfrak{P}'}} \quad \Leftrightarrow \quad I(\mathfrak{P}/\mathfrak{p})\ \sigma\ D(\mathfrak{P}/\mathfrak{P}') = I(\mathfrak{P}/\mathfrak{p})\ \tau\ D(\mathfrak{P}/\mathfrak{P}').$$

(בצד שמאל של המשוואה השניה מדובר בשוויון של מחלקות כפולות של תת חבורות של $\mathrm{Aut}(F/E)$*.)*

(ב) *יהי* $\sigma \in D(\mathfrak{P}/\mathfrak{p})$*. בהנחה ש־*$F/E$ *סופית, מתקיים*

$$\frac{|I(\mathfrak{P}/\mathfrak{p})\ \sigma\ D(\mathfrak{P}/\mathfrak{P}')|}{|D(\mathfrak{P}/\mathfrak{P}')|} = e(\mathfrak{P}'/\mathfrak{p}).$$

הוכחה: (א) לפי ההגדרה $D(\mathfrak{P}/\mathfrak{P}') = \mathrm{Aut}(F/F') \cap D(\mathfrak{P}/\mathfrak{p})$, לכן, עבור $\sigma, \tau \in D(\mathfrak{P}/\mathfrak{p})$:

$$\sigma|_{F'} = \tau|_{F'} \Leftrightarrow \sigma\mathrm{Aut}(F/F') = \tau\mathrm{Aut}(F/F') \Leftrightarrow \sigma D(\mathfrak{P}/\mathfrak{P}') = \tau D(\mathfrak{P}/\mathfrak{P}').$$

ההעתקות $D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Aut}(F_{\mathfrak{P}}/E_{\mathfrak{p}})$, $D(\mathfrak{P}/\mathfrak{P}') \to \mathrm{Aut}(F_{\mathfrak{P}}/F'_{\mathfrak{P}'})$ הן על. לכן

$$\begin{aligned}
\bar{\sigma}|_{F'_{\mathfrak{P}'}} = \bar{\tau}|_{F'_{\mathfrak{P}'}} & \qquad \Big((\bar{\tau}^{-1})|_{F'_{\mathfrak{P}'}}\bar{\sigma}|_{F'_{\mathfrak{P}'}} = \mathrm{id}_{F'_{\mathfrak{P}'}} \Leftrightarrow\Big)\\
\Leftrightarrow \big(\exists\bar{\eta} \in \mathrm{Aut}(F_{\mathfrak{P}}/F'_{\mathfrak{P}'})\big)\bar{\sigma} = \bar{\tau}\bar{\eta} & \qquad \Big((\exists\bar{\eta})\bar{\tau}^{-1}\bar{\sigma} = \bar{\eta} \Leftrightarrow\Big)\\
\Leftrightarrow \big(\exists\eta \in D(\mathfrak{P}/\mathfrak{P}')\big)\bar{\sigma} = \overline{\tau\eta} & \qquad \Big((\exists\eta)\bar{\sigma}(\overline{\tau\eta})^{-1} = 1 \Leftrightarrow\Big)\\
\Leftrightarrow \big(\exists\rho \in I(\mathfrak{P}/\mathfrak{p})\big)\big(\exists\eta \in D(\mathfrak{P}/\mathfrak{P}')\big)\sigma = \rho\tau\eta & \qquad \Big((\exists\rho)(\exists\eta)\sigma(\tau\eta)^{-1} = \rho \Leftrightarrow\Big)\\
\Leftrightarrow \sigma \in I(\mathfrak{P}/\mathfrak{p})\ \tau\ D(\mathfrak{P}/\mathfrak{P}') &\\
\Leftrightarrow I(\mathfrak{P}/\mathfrak{p})\ \sigma\ D(\mathfrak{P}/\mathfrak{P}') = I(\mathfrak{P}/\mathfrak{p})\ \tau\ D(\mathfrak{P}/\mathfrak{P}') &
\end{aligned}$$

(ב) נסמן $I = I(\mathfrak{P}/\mathfrak{p}),\ D = D(\mathfrak{P}/\mathfrak{P}')$. אז $I, D \leq D(\mathfrak{P}/\mathfrak{p})$ ו־$I \cap D = I(\mathfrak{P}/\mathfrak{P}')$.
כיוון ש־$I \lhd D(\mathfrak{P}/\mathfrak{p})$ ו־$\sigma \in D(\mathfrak{P}/\mathfrak{p})$, מתקיים $\sigma^{-1}I\sigma = I$. לכן

$$\frac{|I\sigma D|}{|D|} = \frac{|\sigma^{-1}I\sigma D|}{|D|} = \frac{|ID|}{|D|} = \frac{|I|}{|I \cap D|} = \frac{e(\mathfrak{P}/\mathfrak{p})}{e(\mathfrak{P}/\mathfrak{P}')} = e(\mathfrak{P}'/\mathfrak{p}).$$

∎

21. מחלקים בהרחבות

תהי F/L הרחבת שדות פונקציות של E/K.

הגדרה 21.1: לכל מחלק ראשוני $\mathfrak{p}$ של E/K נתאים מחלק $\sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})\mathfrak{P}$. התאמה זו ניתנת להרחבה להומומורפיזם $\mathrm{Con} = \mathrm{Con}_{F/E} : \mathcal{D}(E/K) \to \mathcal{D}(F/L)$ (**קונורמה**). ∎

למה 21.2: *(א) $\mathrm{Con}_{F/E}$ הוא חד חד ערכי.*

(ב) $\mathfrak{a} \geq 0$ *אם ורק אם* $\mathrm{Con}\,\mathfrak{a} \geq 0$.

(ג) *אם* $\mathfrak{a}, \mathfrak{b} \in \mathcal{D}(E/K)$ *זרים אז* $\mathrm{Con}\,\mathfrak{a}, \mathrm{Con}\,\mathfrak{b}$ *זרים.*

(ד) *תהי* F'/L' *הרחבת שדות פונקציות של* F/L*. אז* $\mathrm{Con}_{F'/E} = \mathrm{Con}_{F'/F} \circ \mathrm{Con}_{F/E}$.

(ה) *יהי* $x \in E^\times$*. אז* $(x)_F = \mathrm{Con}\left((x)_E\right)$, $(x)_{F,0} = \mathrm{Con}\left((x)_{E,0}\right)$, $(x)_{F,\infty} = \mathrm{Con}\left((x)_{E,\infty}\right)$.

(ו) *אם* F/E *סופית, אז* $\deg_F \mathrm{Con}\,\mathfrak{a} = \frac{[F:E]}{[L:K]} \deg_E \mathfrak{a}$.

הוכחה: (ב), (ג), (ד) ברורים.

(א) אם $\mathfrak{p} = \mathfrak{a}$ ראשוני, אז יש מעליו מחלק ראשוני של F/L לפי למה 19.7, ולכן $\mathrm{Con}\,\mathfrak{a} \neq 0$. לכן, אם $0 \neq \mathfrak{a} \in \mathcal{D}(E/K)$ אז $\mathrm{Con}\,\mathfrak{a} \neq 0$ לפי (ג).

(ה) יהי $x \in E^\times$. אז

$$(x)_F = \sum_{\mathfrak{P} \in \mathcal{D}(F/L)} v_{\mathfrak{P}}(x)\mathfrak{P} = \sum_{\mathfrak{p} \in \mathcal{D}(E/K)} \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) v_{\mathfrak{p}}(x)\mathfrak{P} =$$
$$= \sum_{\mathfrak{p} \in \mathcal{D}(E/K)} v_{\mathfrak{p}}(x)\,\mathrm{Con}(\mathfrak{p}) = \mathrm{Con}\Big(\sum_{\mathfrak{p} \in \mathcal{D}(E/K)} v_{\mathfrak{p}}(x)\mathfrak{p}\Big) = \mathrm{Con}\left((x)_E\right)$$

מכאן $(x)_F = \mathrm{Con}\left((x)_{E,0}\right) - \mathrm{Con}\left((x)_{E,\infty}\right)$. לפי (ב), (ג), $\mathrm{Con}\left((x)_{E,0}\right), \mathrm{Con}\left((x)_{E,\infty}\right) \geq 0$ זרים, לכן $(x)_{F,0} = \mathrm{Con}\left((x)_{E,0}\right)$, $(x)_{F,\infty} = \mathrm{Con}\left((x)_{E,\infty}\right)$.

(ו) כיוון ש־$\deg, \mathrm{Con}$ הומומורפיזמים, די להוכיח את השוויון רק עבור $\mathfrak{p} = \mathfrak{a}$ ראשוני. ואכן,

$$\deg \mathrm{Con}\,\mathfrak{p} = \deg \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})\mathfrak{P} = \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{P} = .$$
$$= \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{p} \frac{1}{[L:K]} = \frac{[F:E]}{[L:K]} \deg \mathfrak{p}$$

(השתמשנו במשוואה (2) בפרק 19 ובשוויון היסודי – משפט 19.8). ∎

נזהה $\mathfrak{a} \in \mathcal{D}(E/K)$ עם $\mathrm{Con}\,\mathfrak{a}$. אך כיוון ש־$\mathrm{Con}$ אינה שומרת מעלה, נכתוב $\deg_E \mathfrak{a}, \deg_F \mathfrak{a}$ במקום $\deg \mathrm{Con}\,\mathfrak{a}, \deg \mathfrak{a}$ בהתאמה. בפרט, $\deg_F(x) = \frac{[F:E]}{[L:K]} \deg_E(x)$ לכל $x \in E$. באופן דומה נכתוב $\dim_E \mathfrak{a}, \dim_F \mathfrak{a}$, $\mathcal{L}_E(\mathfrak{a}), \mathcal{L}_F(\mathfrak{a})$, g_E, g_F.

תרגיל 21.4: *אם L/K הרחבה פשוטה (בפרט, אם L/K פרידה סופית) אז* $[F:E]/[L:K] \in \mathbb{N}$.

רמז: השתמש בתרגיל 6.7. ∎

נגדיר כעת העתקה בכיוון ההפוך: הדגש נורמה $\mathrm{Norm}_{F/E} : \mathcal{D}(F/L) \to \mathcal{D}(E/K)$.

יהי E_s ההרחבה הפרידה הגדולה ביותר של E בתוך F. יהי $\hat{F}$ סגור נורמלי של F/E (ההרחבה הנורמלית הקטנה ביותר של E בתוך $\tilde{E} = \tilde{F}$ אשר מכילה את F). אז $\hat{F}/E$ סופית. מתקיים $\hat{F} = F\widehat{E_s}$, כי $\widehat{E_s}/E$ נורמלית ו־$F\widehat{E_s}/\widehat{E_s}$ אי פרידה טהורה, לכן $F\widehat{E_s}/E$ נורמלית.

$$\begin{tikzcd}
\widehat{E_s} \arrow[r, dash] \arrow[d, dash] & F\widehat{E_s} = \hat{F} \arrow[d, dash] \\
E_s \arrow[r, dash] \arrow[d, dash, "\text{פריד}"'] & F \\
E &
\end{tikzcd}$$

היות ו־F/E_s נורמלית נסמן $G = \mathrm{Aut}(\hat{F}/E), H = \mathrm{Aut}(\hat{F}/F)$. יהיו $\sigma_1, \dots, \sigma_r \in G$ מייצגים של G/H, כלומר, $G = \dot{\bigcup}_{i=1}^{r} \sigma_i H$. אז נגדיר

$$\mathrm{Norm}_{F/E}(\mathfrak{a}) = [\hat{F} : E]_i \sum_{i=1}^{r} \sigma_i \mathfrak{a}, \qquad \mathfrak{a} \in \mathcal{D}(F/L)$$

זהו אנלוג של פונקצית הנורמה $\mathrm{Norm}_{F/E} : F \to E$ המוגדרת כך:

$$\mathrm{Norm}_{F/E}(y) = \Big(\prod_{i=1}^{r} \sigma_i y\Big)^{[\hat{F}:E]_i}, \qquad y \in F$$

משפט 21.5: *קיים $0 < \lambda \in \mathbb{Q}$ (שתלוי ב־F/E) כך שלכל $\mathfrak{a} \in \mathcal{D}(E/K)$ מתקיים*

$$\deg_F \mathfrak{a} = \lambda \deg_E \mathfrak{a} \,. \tag{1}$$

אם F/E סופית, אז $\lambda = [F:E]/[L:K]$.

הוכחה: די להוכיח את (1) עבור $\mathfrak{a}$ ראשוני. לשם כך די להוכיח שאם $\mathfrak{p}, \mathfrak{q}$ ראשוניים אז

$$\frac{\deg_E \mathfrak{p}}{\deg_F \mathfrak{p}} = \frac{\deg_E \mathfrak{q}}{\deg_F \mathfrak{q}}.$$

נניח בשלילה שיש $\mathfrak{p}, \mathfrak{q}$ ראשוניים כך ש־$\frac{\deg_E \mathfrak{q}}{\deg_F \mathfrak{q}} < \frac{\deg_E \mathfrak{p}}{\deg_F \mathfrak{p}}$, כלומר, $\frac{\deg_F \mathfrak{p}}{\deg_F \mathfrak{q}} < \frac{\deg_E \mathfrak{p}}{\deg_E \mathfrak{q}}$. אז יש $m, n \in \mathbb{N}$ כך ש־

$$\frac{\deg_E \mathfrak{p}}{\deg_E \mathfrak{q}} < \frac{m}{n} < \frac{\deg_F \mathfrak{p}}{\deg_F \mathfrak{q}}.$$

מכאן

$$0 < \deg_F(n\mathfrak{p} - m\mathfrak{q}), \qquad \deg_E(n\mathfrak{p} - m\mathfrak{q}) < 0 \,.$$

לכן כדי להגיע לסתירה די להוכיח

טענה: *יהי* $\mathfrak{a} \in \mathcal{D}(E/K)$ כך ש־$\deg_E \mathfrak{a} > 0$. אז $\deg_F \mathfrak{a} \geq 0$.

אכן, יהי $k \in \mathbb{N}$ גדול מספיק. אז לפי רימן־רוך $\dim k\mathfrak{a} = k \deg \mathfrak{a} + 1 - g_E > 0$, לכן יש $x \in E^\times$ כך ש־$(x)_E + k\mathfrak{a} \geq 0$. אז גם $(x)_F + k \operatorname{Con} \mathfrak{a} = \operatorname{Con}\left((x)_E + k\mathfrak{a}\right) \geq 0$, ולכן $\deg \operatorname{Con} \mathfrak{a} = \frac{1}{k} \deg\left((x)_F + k \operatorname{Con} \mathfrak{a}\right) \geq 0$. ∎

22. הרחבת שדה המקדמים

הגדרה 22.1: הרחבה F/L של שדה פונקציות E/K נקראת **הרחבת שדה המקדמים** אם $F = LE$. ∎

$$\begin{tikzcd}
E \arrow[r, dash] \arrow[d, dash] & F \arrow[d, dash] \\
K \arrow[r, dash] & L
\end{tikzcd}$$

דוגמה 22.2: יש שדה פונקציות אלגבריות במשתנה אחד E/K ויש הרחבה אי פרידה טהורה (ממעלה ראשונית) L/K כך ש־EL/L אינו כלל שדה פונקציות.

אכן, יהי K בעל אפיון 2 ויהיו $a, b \in K$ כך ש־$\sqrt{a}, \sqrt{b}$ יוצרים שתי הרחבות ריבועיות שונות של K. (למשל, $K = \mathbb{F}_2(a, b)$, באשר a, b בלתי תלויים אלגברית מעל $\mathbb{F}_2$.) אז $[K(\sqrt{a}, \sqrt{b}) : K] = 4$. יהי x טרנסצנדנטי מעל K ויהי $y \in \widetilde{K(x)}$ שמקיים $y^2 = ax^2 + b$. אז קיים התרשים הבא של שדות ומעלות ההרחבות

$$\begin{tikzcd}
K(x,y) \arrow[r, dash, "2"] \arrow[d, dash, "2"'] & K(\sqrt{a},x,y) \arrow[r, equal] \arrow[d, dash, "2"'] & K(\sqrt{a},\sqrt{b},x,y) \arrow[d, equal] \\
K(x) \arrow[r, dash, "2"] \arrow[d, dash] & K(\sqrt{a},x) \arrow[r, dash, "2"] \arrow[d, dash] & K(\sqrt{a},\sqrt{b},x) \arrow[d, dash] \\
K \arrow[r, dash, "2"] & K(\sqrt{a}) \arrow[r, dash, "2"] & K(\sqrt{a},\sqrt{b})
\end{tikzcd}$$

כי, בין היתר, $y = \sqrt{a}x + \sqrt{b}$.

טענה 1: *$K(x,y)/K$ שדה פונקציות, דהיינו, K סגור אלגברית בתוך $K(x,y)$.*

אכן, $1, \sqrt{a}$ בסיס של $K(\sqrt{a})$ מעל K, ו־$1, \sqrt{b}$ בסיס של $K(\sqrt{a}, \sqrt{b})$ מעל $K(\sqrt{a})$, לכן $1, \sqrt{a}, \sqrt{b}, \sqrt{a}\sqrt{b}$ בסיס של $K(\sqrt{a}, \sqrt{b})$ מעל K.

מאותם הנימוקים $1, \sqrt{a}, \sqrt{b}, \sqrt{a}\sqrt{b}$ בסיס של $K(\sqrt{a}, \sqrt{b}, x)$ מעל $K(x)$.

יהי $\alpha \notin K$ אלגברי מעל K ונניח ש־$\alpha \in K(x,y)$. אז $\alpha \in K(\sqrt{a}, \sqrt{b}, x, y) = K(\sqrt{a}, \sqrt{b}, x)$ ולכן $\alpha = c_0 + c_1\sqrt{a} + c_2\sqrt{b} + c_3\sqrt{a}\sqrt{b}$, באשר $c_i \in K$.

לפי תרגיל 6.7, $K(x, \alpha)$ הרחבה נאותה של $K(x)$. היא מוכלת ב־$K(x,y)$, לכן $K(x,y) = K(x,\alpha)$. מכאן $y \in K(x,\alpha)$. כיוון ש־$1, \alpha$ הוא בסיס של $K(x,\alpha)$ מעל $K(x)$, יש $f(x), g(x) \in K(x)$ כך ש־

$$y = f(x) + g(x)\alpha = f(x) + g(x)(c_0 + c_1\sqrt{a} + c_2\sqrt{b} + c_3\sqrt{a}\sqrt{b}) =$$

$$= (f(x) + g(x)c_0) + c_1 g(x)\sqrt{a} + c_2 g(x)\sqrt{b} + c_3 g(x)\sqrt{a}\sqrt{b}$$

אבל גם $y=\sqrt{a}x+\sqrt{b}$. מיחידות ההצגה נובע $c_2g(x)=1$, כלומר, $g(x)=c_2^{-1}\in K$, ו־$c_1g(x)=x$, כלומר, $g(x)=c_1^{-1}x\notin K$, סתירה. בכך הוכחה הטענה.

טענה 2: $K(\sqrt{a},x,y)/K(\sqrt{a})$ *אינה שדה פונקציות.* אכן, $\sqrt{b}\in\widetilde{K(\sqrt{a})}\cap K(\sqrt{a},x,y)$, אבל $\sqrt{b}\notin K(\sqrt{a})$. לכן $K(\sqrt{a})$ אינו סגור אלגברית בתוך $K(\sqrt{a},x,y)$. ∎

נוכיח שדבר זה אינו קורה אם L/K פרידה. לשם כך נזדקק ללמה:

למה 22.3: *תהי M/K הרחבת שדות סופית, $\mathrm{char}\ K=p>0$, $[M:K]_i=p$. אז ל־M/K יש איבר פרימיטיבי.*

הוכחה: די להוכיח שלהרחבה M/K רק מספר סופי של שדות ביניים. (זה שקול לכך שיש איבר פרימיטיבי.)

טענה: *ל־K יש לכל היותר הרחבה אי פרידה טהורה נאותה אחת מוכלת ב־M.* אכן, אם K_1,K_2 כאלה ושונות, אז K_1K_2/K אי פרידה טהורה, $[K_1K_2:K]>p$, לכן $[K_1K_2:K]_i=[K_1K_2:K]\nmid[M:K]_i$, סתירה.

יהי M_0 הסגור הפריד של K בתוך M.

יהי E שדה ביניים של M/K. יהי E_0 הסגור הפריד של K בתוך E. אז $E_0\subseteq M_0$ ו־E/E_0 אי פרידה טהורה. כמו כן $[M:E_0]_i=\frac{[M:K]_i}{[E_0:K]_i}=\frac{p}{1}=p$. לכן לפי הטענה יש ל־$E_0$ לכל היותר שתי הרחבות אי פרידות טהורות (אחת טריביאלית) מוכלות ב־M. כיוון של־M_0/K רק מספר סופי של שדות ביניים, טענת הלמה ברורה. ∎

$$\begin{tikzcd}
 & M \\
E \arrow[r, dash] \arrow[d, dash] & EM_0 \arrow[u, dash] \arrow[d, dash] \\
E_0 \arrow[r, dash, "\text{פריד}"] \arrow[d, dash, "\text{פריד}"'] & M_0 \\
K &
\end{tikzcd}$$

משפט 22.4: *יהי E/K שדה פונקציות ותהי L/K הרחבה פרידה סופית. אז LE/L שדה פונקציות.*

הוכחה: די להוכיח שאם M/L סופית נאותה, אז $M\not\subseteq EL$. לשם כך די להניח, של־M/L אין שדות ביניים (אחרת נחליף M בשדה ביניים). לכן M/L פרידה או אי פרידה טהורה ממעלה p.

במקרה הראשון M/K פרידה סופית ובמקרה השני $[M:K]_i=p$. לפי משפט ידוע ולפי הלמה, יש ל־M/K איבר פרימיטיבי β. יהי f הפולינום האי פריק המתוקן שלו מעל K. לפי תרגיל 6.7, f אי פריק מעל E. לכן $[ME:E]=\deg f=[M:K]>[L:K]\geq[LE:E]$. לכן $ME\not\subseteq LE$ ומכאן $M\not\subseteq LE$. ∎

$$\begin{tikzcd}
E \arrow[r, dash] & LE \arrow[r, dash] & ME \\
K \arrow[r, dash] \arrow[u, dash] & L \arrow[r, dash] \arrow[u, dash] & M \arrow[u, dash]
\end{tikzcd}$$

נניח מעתה כי F/L הרחבת שדה המקדמים של E/K, באשר L/K פרידה סופית.

משפט 22.5: *(א)* $[F:E]=[L:K]$.

(ב) $\deg_F \mathfrak{a} = \deg_E \mathfrak{a}$ *לכל* $\mathfrak{a}\in\mathcal{D}(E/K)$.

הוכחה: (א) יש $\alpha\in L$ כך ש־$L=K(\alpha)$. אז $F=LE=E(\alpha)$. לפי תרגיל 6.7,
$[F:E]=\deg\operatorname{irr}(\alpha,K)=[L:K]$.

(ב) נובע מ־(א) לפי למה 21.2(ו). ∎

משפט 22.6: *יהי* $\mathfrak{P}$ *מחלק ראשוני של* F/L *ויהי* $\mathfrak{p}$ *המחלק הראשוני של* E/K *המונח תחתיו. אז* $F_{\mathfrak{P}}=LE_{\mathfrak{p}}$.

הוכחה: $L,E_{\mathfrak{p}}\subseteq F_{\mathfrak{P}}$, לכן די להוכיח $F_{\mathfrak{P}}\subseteq LE_{\mathfrak{p}}$. יהי $\bar z\in F_{\mathfrak{P}}$.

יהי $\hat L$ סגור גלואה של L/K. יהי $\hat{\mathfrak{P}}$ מחלק ראשוני של $\hat F=\hat L E$ שמונח מעל $\mathfrak{P}$.

טענה 1: *קיים ל־$\bar z$ מייצג $z\in\mathcal{O}_{\mathfrak{P}}$ כך ש־$\sigma z\in\mathcal{O}_{\hat{\mathfrak{P}}}$ לכל $\sigma\in\operatorname{Gal}(\hat F/E)$.* אכן, (כמו בהוכחה של משפט 20.7) יהי $z'\in\mathcal{O}_{\mathfrak{P}}$ מייצג כלשהו. לפי משפט הקירוב החלש יש $z\in F$ כך ש־$v_{\mathfrak{P}}(z-z')>0$ (ובפרט $v_{\mathfrak{P}}(z)\ge 0$, כלומר, $z\in\mathcal{O}_{\mathfrak{P}}$, ו־$z$ מייצג את $\bar z$) ו־$v_{\mathfrak{P}'}(z)\ge 0$ לכל מחלק ראשוני $\mathfrak{P}'$ של F שמונח מעל $\mathfrak{p}$ ושונה מ־$\mathfrak{P}$. אז $v_{\hat{\mathfrak{P}}'}(z)\ge 0$ לכל מחלק ראשוני $\hat{\mathfrak{P}}'$ של $\hat F$ שמונח מעל $\mathfrak{p}$, כלומר, $v_{\hat{\mathfrak{P}}}(\sigma z)=v_{\sigma^{-1}\hat{\mathfrak{P}}}(z)\ge 0$ לכל $\sigma\in\operatorname{Gal}(\hat F/E)$. בכך הוכחה הטענה.

יהי $n=[L:K]$ ויהי α איבר פרימיטיבי עבור L/K. אז $1,\alpha,\dots,\alpha^{n-1}$ בסיס של L מעל K.

טענה 2: *יהי $z\in F$. יהיו $\sigma_0,\dots,\sigma_{n-1}$ כל השיכונים של F לתוך $\hat F$ מעל E. אז יש $x_0,\dots,x_{n-1}\in E\cap\operatorname{Span}_{\hat L}(\sigma_0 z,\dots,\sigma_{n-1}z)\subseteq\hat F$ כך ש־*

$$z=\sum_{j=0}^{n-1}x_j\alpha^j. \tag{1}$$

מתקיים $F=EL=E(\alpha)$, לכן לפי תרגיל 6.7, $1,\alpha,\dots,\alpha^{n-1}$ גם בסיס של F מעל E. לכן קיימים $x_0,\dots,x_{n-1}\in E$ כך שמתקיים (1). מכאן

$$\sigma_i z=\sum_{j=0}^{n-1}x_j(\sigma_i\alpha^j),\qquad i=0,\dots,n-1. \tag{2}$$

זוהי מערכת של n משוואות לינאריות ב־$x_0,\dots,x_{n-1}$ מעל $\hat L$. המטריצה שלה $A=(\sigma_i\alpha^j)\in\mathrm{M}_n(\hat L)$ הפיכה, כי L/K פרידה. (הדטרמיננטה של מטריצה זו היא דטרמיננטת ונדרמונדה $\Delta=\prod_{j<l}(\sigma_l\alpha-\sigma_j\alpha)\neq 0$.) תהי $B=(b_{ji})\in\mathrm{M}_n(\hat L)$ ההופכית של A. אז

$$E\ni x_j=\sum_i b_{ji}\sigma_i z\in\operatorname{Span}_{\hat L}(\sigma_0 z,\dots,\sigma_{n-1}z),\qquad j=0,\dots,n-1.$$

בכך הוכחה הטענה.

אך $\sigma_0 z, \dots, \sigma_{n-1} z \in \mathcal{O}_{\hat{\mathfrak{P}}}$ ו־$\hat{L} \subseteq \mathcal{O}_{\hat{\mathfrak{P}}}$, לכן $x_0, \dots, x_{n-1} \in E \cap \mathcal{O}_{\hat{\mathfrak{P}}} = \mathcal{O}_{\mathfrak{p}}$. לפי (1), $\bar{z} = \sum_{j=0}^{n-1} \bar{x}_j \alpha^j \in E_{\mathfrak{p}} L$. ∎

תרגיל 22.7: *הרחב את מסקנת המשפט הקודם גם ל־L/K פרידה (אלגברית) אינסופית.*

תרגיל 22.8: *יהי E/K שדה פונקציות. נניח ש־K משוכלל (כל הרחבה סופית שלו פרידה). הראה שיש L/K סופית כך שלהרחבת שדה המקדמים LE/L יש מחלק ראשוני בעל מעלה 1.*

תרגיל 22.9: *תהיינה M_1, M_2 שתי הרחבות של שדה K מוכלות בשדה משותף M. נניח כי*

(א) *כל קבוצה $A_1 \subseteq M_1$ בלתי תלויה לינארית מעל K הינה גם בלתי תלויה (כתת קבוצה של M) מעל M_2.*

אז

(ב) *כל קבוצה $A_2 \subseteq M_2$ בלתי תלויה לינארית מעל K הינה גם בלתי תלויה (כתת קבוצה של M) מעל M_1.*

הסק (בתנאים של הפרק) שכל קבוצה $A \subseteq E$ בלתי תלויה לינארית מעל K הינה גם בלתי תלויה לינארית מעל L.

הוכחה: יהיו $y_1, \dots, y_n \in M_2$ בלתי תלויים לינארית מעל K. יהיו $\alpha_1 \dots, \alpha_n \in M_1$ כך ש־$\sum_{i=1}^n \alpha_i y_i = 0$. נבחר בסיס $x_1, \dots, x_m \in M_1$ של $\mathrm{Span}_K(\alpha_1, \dots, \alpha_n) \subseteq M_1$ מעל K. אז $\alpha_i = \sum_{k=1}^m b_{ik} x_k$ לכל i. מכאן

$$0 = \sum_{i=1}^n \Big(\sum_{k=1}^m b_{ik} x_k\Big) y_i = \sum_{k=1}^m \Big(\sum_{i=1}^n b_{ik} y_i\Big) x_k.$$

לפי ההנחה $x_1, \dots, x_m$ בלתי תלויים לינארית מעל M_2, לכן $\sum_{i=1}^n b_{ik} y_i = 0$ לכל k. מכאן $b_{ik} = 0$ לכל i, k, כי $y_1, \dots, y_n$ בלתי תלויים לינארית מעל K. לכן $\alpha_i = \sum_{k=1}^m b_{ik} x_k = 0$ לכל i.

$$\begin{tikzcd}
M_2 \arrow[r, dash] \arrow[d, dash] & M \arrow[d, dash] \\
K \arrow[r, dash] & M_1
\end{tikzcd}$$

נניח כעת כי E/K שדה פונקציות אלגבריות במשתנה אחד ו־L/K פרידה סופית, נאמר, $[L : K] = n$; יהי $F = EL$. יהי $\alpha \in L$ איבר פרימיטיבי עבור L/K. אז $F = EL = E(\alpha)$ ו־$[F : E] = n$. לכן $1, \alpha, \dots, \alpha^{n-1}$ בסיס של L מעל K וגם בסיס של F מעל E.

אם $\beta_1, \dots, \beta_m$ סדרה של אברי L בלתי תלויה לינארית מעל K, נשלים אותה לבסיס $\beta_1, \dots, \beta_n$ של L מעל K. אז מטריצת המעבר מ־$1, \alpha, \dots, \alpha^{n-1}$ ל־$\beta_1, \dots, \beta_n$ היא מטריצה הפיכה מעל K. בגלל שהיא גם הפיכה כמטריצה מעל E, הסדרה $\beta_1, \dots, \beta_n$ בסיס של F מעל E. בפרט, $\beta_1, \dots, \beta_m$ בלתי תלויה לינארית מעל E. ∎

הוכחנו:

(א) כל קבוצה $A_1 \subseteq L$ בלתי תלויה לינארית מעל K הינה גם בלתי תלויה (כתת קבוצה של F) מעל E.

לכן, לפי התרגיל,

(ב) כל קבוצה $A_2 \subseteq E$ בלתי תלויה לינארית מעל K הינה גם בלתי תלויה (כתת קבוצה של F) מעל L.

$$\begin{tikzcd} E \arrow[r, dash] \arrow[d, dash] & F \arrow[d, dash] \\ K \arrow[r, dash] & L \end{tikzcd} \qquad \blacksquare$$

משפט 22.10: *יהי $\mathfrak{a}$ מחלק של E/K. אז*

(א) $\mathcal{L}_F(\mathfrak{a}) = L\mathcal{L}_E(\mathfrak{a}) := \mathrm{Span}_L\left(\mathcal{L}_E(\mathfrak{a})\right)$.

(ב) $\dim_F \mathfrak{a} = \dim_E \mathfrak{a}$.

הוכחה: ברור ש־ $\mathcal{L}_E(\mathfrak{a}) = \{x \in E \mid (x) + \mathfrak{a} \geq 0\} \subseteq \{x \in F \mid (x) + \mathfrak{a} \geq 0\} = \mathcal{L}_F(\mathfrak{a})$ ו־$\mathcal{L}_F(\mathfrak{a})$ הוא מרחב וקטורי מעל L, לכן

(ג) $L\mathcal{L}_E(\mathfrak{a}) \subseteq \mathcal{L}_F(\mathfrak{a})$.

לפי תרגיל 22.9, בסיס של $\mathcal{L}_E(\mathfrak{a})$ מעל K הוא גם בסיס של $L\mathcal{L}_E(\mathfrak{a})$ מעל L. לכן

(ד) $\dim_E \mathfrak{a} \leq \dim_F \mathfrak{a}$,

(ב) נובע מ־(א), ודי להוכיח כי $\mathcal{L}_F(\mathfrak{a}) \subseteq L\mathcal{L}_E(\mathfrak{a})$.

יהי $z \in \mathcal{L}_F(\mathfrak{a})$. יהי $\hat{L}$ סגור גלואה של L/K, ויהי $\hat{F} = \hat{L}E$, ויהי $\sigma \in \mathrm{Gal}(\hat{F}/E)$.

טענה: $\sigma z \in \mathcal{L}_{\hat{F}}(\mathfrak{a})$. אכן, $(z) + \mathfrak{a} \geq 0$ כמחלק של $\hat{F}/\hat{L}$, כלומר, $v_{\hat{\mathfrak{P}}}(z) + v_{\hat{\mathfrak{P}}}(\mathfrak{a}) \geq 0$ לכל מחלק ראשוני $\hat{\mathfrak{P}}$ של $\hat{F}/\hat{L}$. בפרט $v_{\sigma^{-1}\hat{\mathfrak{P}}}(z) + v_{\sigma^{-1}\hat{\mathfrak{P}}}(\mathfrak{a}) \geq 0$. לכל $\hat{\mathfrak{P}}$

$$v_{\hat{\mathfrak{P}}}(\mathfrak{a}) = e(\hat{\mathfrak{P}}/\mathfrak{p})v_{\mathfrak{p}}(\mathfrak{a}) = e(\sigma^{-1}\hat{\mathfrak{P}}/\mathfrak{p})v_{\mathfrak{p}}(\mathfrak{a}) = v_{\sigma^{-1}\hat{\mathfrak{P}}}(\mathfrak{a}),$$

באשר $\mathfrak{p}$ המחלק של E/K המונח מתחת ל־$\hat{\mathfrak{P}}$. לכן

$$v_{\hat{\mathfrak{P}}}(\sigma z) + v_{\hat{\mathfrak{P}}}(\mathfrak{a}) = v_{\sigma^{-1}\hat{\mathfrak{P}}}(z) + v_{\sigma^{-1}\hat{\mathfrak{P}}}(\mathfrak{a}) \geq 0$$

כלומר, $(\sigma z) + \mathfrak{a} \geq 0$, לכן $\sigma z \in \mathcal{L}_{\hat{F}}(\mathfrak{a})$.

לפי טענה 2 בהוכחת משפט 22.6

$$z = \sum_{j=1}^{n} a_j x_j, \tag{1}$$

באשר $a_1, \ldots, a_n \in L$ ו־ $x_1, \ldots, x_n \in E \cap \mathrm{Span}_{\hat{L}}(\sigma_1 z, \ldots, \sigma_n z) \subseteq E \cap \mathcal{L}_{\hat{F}}(\mathfrak{a}) = \mathcal{L}_E(\mathfrak{a})$. לכן $z \in L\mathcal{L}_E(\mathfrak{a})$. ∎

משפט 22.11: $g_F = g_E$.

הוכחה: יהי $\mathfrak{p}$ מחלק ראשוני של E/K ויהי $k \in \mathbb{N}$ גדול מספיק. יהי $\mathfrak{a} = k\mathfrak{p}$. אז

$$\deg_E \mathfrak{a}, \deg_F \mathfrak{a} \geq k \geq 2g_E - 2, 2g_F - 2 \, .$$

לכן לפי משפט רימן רוך

$$\dim_E \mathfrak{a} = \deg_E \mathfrak{a} + 1 - g_E$$

$$\dim_F \mathfrak{a} = \deg_F \mathfrak{a} + 1 - g_F \, .$$

לפי משפט 22.5(ב), $\deg_E \mathfrak{a} = \deg_F \mathfrak{a}$; לפי משפט 22.10(ב), $\dim_E \mathfrak{a} = \dim_F \mathfrak{a}$. לכן $g_E = g_F$. ∎

23. סיעוף

תהי F/L הרחבה של שדה פונקציות E/K.

הגדרה 23.1: יהי $\mathfrak{P}$ מחלק ראשוני של F/L ויהי $\mathfrak{p}$ המחלק הראשוני של E/K המונח מתחתיו. אז $\mathfrak{P}$

(א) **אינו מסועף מעל** E אם $e(\mathfrak{P}/\mathfrak{p}) = 1$,

(א) **פריד מעל** E אם הרחבת שדות השאריות $F_{\mathfrak{P}}/E_{\mathfrak{p}}$ פרידה. ∎

למה 23.2: *נניח כי F/E גלואה סופית. אז $\mathfrak{P}$ אינו מסועף והינו פריד מעל E אם ורק אם $I(\mathfrak{P}/\mathfrak{p}) = 1$.*

הוכחה: לפי מסקנה 20.11(ג), $|I(\mathfrak{P}/\mathfrak{p})| = e(\mathfrak{P}/\mathfrak{p})[F_{\mathfrak{P}} : E_{\mathfrak{p}}]_i$. לכן $I(\mathfrak{P}/\mathfrak{p}) = 1$ אם ורק אם $e(\mathfrak{P}/\mathfrak{p}) = 1, [F_{\mathfrak{P}} : E_{\mathfrak{p}}]_i = 1$. ∎

למה 23.3: *נניח כי L/K פרידה סופית ו־$F = LE$. אז כל מחלק ראשוני $\mathfrak{P}$ של F/L אינו מסועף והינו פריד מעל E.*

הוכחה: נסמן $\mathfrak{p} = E \cap \mathfrak{P}$, המחלק הראשוני של E/K המונח מתחת ל־$\mathfrak{P}$. די להוכיח את הטענה להרחבה פרידה גדולה יותר, למשל סגור גלואה של L/K, ולכן בלי הגבלת הכלליות L/K גלואה. אז גם F/E גלואה. לפי הלמה הקודמת די להוכיח כי אם $\sigma \in I(\mathfrak{P}/\mathfrak{p})$ אז $\sigma = 1$.

ואכן, $\sigma|_E = 1$. יהי $b \in L$. אז גם $\sigma b \in L$. לפי הגדרת $I(\mathfrak{P}/\mathfrak{p})$, $\bar{b} = \overline{\sigma b}$. האתר המתאים ל־$\mathfrak{P}$ הוא הזהות על L, לכן $\bar{b} = b, \overline{\sigma b} = \sigma b$. מכאן $\sigma b = b$. לכן $\sigma|_L = 1$. כיוון ש־$F = EL$, $\sigma = 1$. ∎

$$\begin{array}{ccccc} E & \text{——} & F & \text{——} & \hat{F} \\ | & & | & & | \\ K & \text{——} & L & \text{——} & \hat{L} \end{array}$$

24. פונקצית זיתא של רימן

בפרקים הבאים נדבר על ספירה של מחלקים ראשוניים ופונקצית זיתא מעל שדות סופיים, אנלוג של פונקצית זיתא הקלאסית של רימן. כאן נדבר בקצרה על המקרה הקלאסי.

פונקצית זיתא של רימן מוגדרת בשלבים. קודם כל,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad s \in \mathbb{C},\ \operatorname{Re} s > 1.$$

הטור מתכנס בהחלט, ומגדיר פונקציה הולומורפית בתחום הנ"ל.

הפירוק של מספרים טבעיים למכפלה של מספרים ראשוניים נותן את ההצגה הבאה (מכפלת אוילר)

$$\zeta(s) = \prod_{p\ \text{ראשוני}} \frac{1}{1-p^s} \quad \Big(= \prod_{p\ \text{ראשוני}} \Big(\sum_{k=0}^{\infty} \frac{1}{p^{ks}}\Big)\Big), \qquad s \in \mathbb{C},\ \operatorname{Re} s > 1$$

(כאשר p עובר על כל המספרים הראשוניים) ממנה רואים של־ζ אין אפסים בַּתחום.

אפשר להמשיך את ζ לפונקציה מירומורפית על כל המישור המרוכב:

(א) $\zeta(s) = (1-\frac{2}{2^s})^{-1}\eta(s)$, עבור $\operatorname{Re} s > 1$, באשר $\eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$ הולומורפית עבור $\operatorname{Re} s > 0$.
לכן נרחיב את הגדרת $\zeta(s)$ על ידי המשוואה גם עבור $\operatorname{Re} s > 0$.

(ב) בתחום $0 < \operatorname{Re} s < 1$ מתקיימת **המשוואה הפונקציונלית**

$$\zeta(s) = 2^s \pi^{s-1} \sin\big(\frac{\pi s}{2}\big)\Gamma(1-s)\zeta(1-s).$$

בעזרתה נרחיב את ההגדרה עבור $\operatorname{Re} s < 1$ כלשהו.

ל־ζ יש קוטב יחיד בנקודה $s = 1$ והוא פשוט. יש לה אפסים (פשוטים) בנקודות $-2, -4, -6, \ldots$. אלה נקראים **אפסים טריביאליים**. אין ל־ζ אפסים מחוץ לתחום $0 < \operatorname{Re} s < 1$. **השערת רימן** אומרת שכל האפסים הנוספים (הלא טריביאליים) מקיימים $\operatorname{Re} s = \frac{1}{2}$.

זוהי אולי ההשערה המתמטית החשובה ביותר. ממנה נובעות השערות רבות מתורת המספרים והיא נותנת הערכה טובה למספר המספרים הראשוניים הקטנים ממספר נתון (**משפט המספרים הראשוניים**).

25. פונקצית זיתא

נקבע את הסימון הבא:

K שדה סופי,

$p = \mathrm{char}\ K$,

q מספר אברי K; זוהי חזקה של p,

F שדה פונקציות אלגבריות במשתנה אחד מעל K,

$g = g_F$ הגזע של F/K,

$\mathbb{P}$ קבוצת המחלקים הראשוניים של F/K,

$\mathcal{D}$ חבורת המחלקים של F/K,

$\mathcal{C} = \mathcal{D}/\{(x)|\ x \in F^\times\}$ חבורת מחלקות המחלקים,

$\mathcal{C}_m = \{\mathfrak{a} \in \mathcal{D}|\ \deg \mathfrak{a} = m\}/\{(x)|\ x \in F^\times\}$,

$h = |\mathcal{C}_0|$ (נראה מיד ש־$h < \infty$),

$\partial = \min(\deg \mathfrak{b}|\ \mathfrak{b} \in \mathcal{D},\ \deg \mathfrak{b} > 0)$ (מאוחר יותר נוכיח כי $\partial = 1$),

$A_n := |\{\mathfrak{b}|\ \deg \mathfrak{b} = n,\ \mathfrak{b} \geq 0\}|$.

אם $\mathfrak{a}, \mathfrak{b} \in \mathcal{D}$ ו־$\mathfrak{b} \sim \mathfrak{a}$ אז $\deg \mathfrak{a} = \deg \mathfrak{b}$ ו־$\dim \mathfrak{a} = \dim \mathfrak{b}$ (מסקנה 7.8). לכן לכל מחלקה $C \in \mathcal{C}$ אפשר להגדיר $\dim C = \dim \mathfrak{a}$, $\deg C = \deg \mathfrak{a}$, באשר $\mathfrak{a} \in C$.

למה 25.1: *לכל $m \in \mathbb{Z}$ הקבוצות הבאות סופיות:*

(א) $S_m(F) = \{\mathfrak{p} \in \mathbb{P}|\ \deg \mathfrak{p} \leq m\}$,

(ב) $\{\mathfrak{a} \in \mathcal{D}|\ \mathfrak{a} \geq 0,\ \deg \mathfrak{a} \leq m\}$,

(ג) $\mathcal{C}_m$*, ובפרט* $\mathcal{C}_0$*; לכן* $h < \infty$.

הוכחה: (א) נניח תחילה כי $F = K(x)$ שדה הפונקציות הרציונליות מעל K. אז $S_m(F) \setminus \{\infty\}$ בהתאמה חד חד ערכית עם קבוצת הפולינומים האי פריקים המתוקנים ב־$K[x]$ ממעלה $\leq m$, שהינה סופית (כי K סופי).

במקרה הכללי יהי $x \in F \setminus K$ ויהי $E = K(x)$. לכל $\mathfrak{p} \in S_m(F)$ יהי $\mathfrak{q}$ המחלק של E/K שמונח מתחתיו. אז $\mathfrak{q} \in S_m(E)$, כי $K \subseteq E_\mathfrak{q} \subseteq F_\mathfrak{p}$ ולכן $\deg \mathfrak{q} \leq \deg \mathfrak{p}$. לפי הפסקה הקודמת $S_m(E)$ סופית; מעל כל $\mathfrak{q} \in S_m(E)$ יש רק מספר סופי של מחלקים של F/K (למה 19.7). לכן $S_m(F)$ סופית.

(ב) אם $\mathfrak{a} \geq 0$ ו־$\deg \mathfrak{a} \leq m$ אז $\mathfrak{a}$ הוא סכום של $\leq m$ מחלקים ראשוניים ממעלה $\leq m$. לכן הטענה נובעת מ־(א).

(ג) נניח תחילה כי $m \geq 2g$. יהי $[\mathfrak{a}] \in \mathcal{C}_m$. לפי משפט רימן־רוך, $\dim \mathfrak{a} = \deg \mathfrak{a} + 1 - g \geq 1$, לכן יש $x \in F^\times$ כך ש־$\mathfrak{a}' := (x) + \mathfrak{a} \geq 0$. כלומר, $\mathfrak{a}' \geq 0$, $[\mathfrak{a}'] = [\mathfrak{a}]$. לכן הטענה נובעת לפי (ב).

במקרה הכללי נבחר מחלק $\mathfrak{b}$ כך ש־$d = \deg \mathfrak{b}$ גדול מאד. אז $\mathfrak{a} \mapsto \mathfrak{a} + \mathfrak{b}$ היא התאמה חד חד ערכית $\{\mathfrak{a}|\ \deg \mathfrak{a} = m\} \to \{\mathfrak{a}'|\ \deg \mathfrak{a}' = m + d\}$ והיא משרה התאמה חד חד ערכית $\mathcal{C}_m \to \mathcal{C}_{d+m}$. לפי הפסקה

הקודמת $\mathcal{C}_{d+m}$ סופית. לכן $\mathcal{C}_m$ סופית. ∎

תרגיל 25.2: *יהי* $n \in \mathbb{Z}$. *אז*

(א) *יש* $\mathfrak{b} \in \mathcal{D}$ *כך ש־* $\deg \mathfrak{b} = n$ *אם ורק אם* $\partial | n$.

(ב) $|\mathcal{C}_n| = \begin{cases} h & \partial | n \\ 0 & \text{אחרת} \end{cases}$.

(ג) $\partial | 2g - 2$.

הוכחה: (א) יש $\mathfrak{b}_0 \in \mathcal{D}$ כך ש־$\deg \mathfrak{b}_0 = \partial$. לפי החילוק עם שארית $n = k\partial + r$, באשר $0 \leq r < \partial$.

נניח כי $\partial | n$, כלומר, $r = 0$. אז $\deg k\mathfrak{b}_0 = n$. להיפך, אם יש $\mathfrak{b} \in \mathcal{D}$ כך ש־$\deg \mathfrak{b} = n$, אז $\deg(\mathfrak{a} - k\mathfrak{b}_0) = r$. לפי המזעריות של ∂ מתקיים $r = 0$. לכן $\partial | n$,

(ב) לפי ההוכחה של הלמה, $|\mathcal{C}_n| = |\mathcal{C}_0| = h$, אם יש מחלק ממעלה n. אם אין, אז, כמובן, $\mathcal{C}_n = \emptyset$.

(ג) יהי $\mathfrak{w}$ מחלק קנוני של F/K. לפי (א), $\partial | 2g - 2 = \deg \mathfrak{w}$. ∎

למה 25.3: *יהי* $\mathfrak{a} \in \mathcal{D}$. *אז* $\frac{q^{\dim \mathfrak{a}} - 1}{q - 1} = |\{\mathfrak{b} | \ \mathfrak{b} \geq 0, \ \mathfrak{b} \sim \mathfrak{a}\}|$.

הוכחה: אם $\mathfrak{a} \sim \mathfrak{b}$, יש $x \in F^\times$ כך ש־$\mathfrak{b} = \mathfrak{a} + (x)$. אם גם $\mathfrak{b} \geq 0$ אז $x \in \mathcal{L}(\mathfrak{a})$. להיפך, אם $0 \neq x \in \mathcal{L}(\mathfrak{a})$ אז $\mathfrak{a} \sim \mathfrak{b} := \mathfrak{a} + (x) \geq 0$. לכן העוצמה המבוקשת היא העוצמה של $\{(x) | \ x \in \mathcal{L}(\mathfrak{a}), \ x \neq 0\}$.

כעת, $|\mathcal{L}(\mathfrak{a})| = q^{\dim \mathfrak{a}}$, לכן $|\mathcal{L}(\mathfrak{a}) \smallsetminus \{0\}| = q^{\dim \mathfrak{a}} - 1$, ו־$(x) = (x')$ אם ורק אם $\frac{x'}{x} \in K^\times$. כלומר, $q - 1$ איברים שונים מגדירים אותו מחלק. מכאן המסקנה. ∎

למה 25.3 (ניסוח שקול): *תהי* $C \in \mathcal{C}$. *אז* $\frac{q^{\dim C} - 1}{q - 1} = |\{\mathfrak{b} \in C | \ \mathfrak{b} \geq 0\}|$.

נזכיר שהגדרנו

$$A_n := |\{\mathfrak{b} \in \mathcal{D} | \ \deg \mathfrak{b} = n, \ \mathfrak{b} \geq 0\}|. \qquad (1)$$

מסקנה 25.4: *(א)* $A_n = \sum_{C \in \mathcal{C}_n} \frac{q^{\dim C} - 1}{q - 1}$.

(ב) *בפרט, אם* $n > 2g - 2$ *אז* $A_n = \begin{cases} h\frac{q^{n+1-g} - 1}{q - 1} & \partial | n \\ 0 & \text{אחרת} \end{cases}$.

הוכחה: (ב) נובע מ־(א) לפי משפט רימן־רוך. ∎

הגדרה 25.5: לכל $\mathfrak{a} \in \mathcal{D}$ נגדיר את **הנורמה** (**המוחלטת**) של $\mathfrak{a}$ על ידי

$$N\mathfrak{a} = q^{\deg \mathfrak{a}}.$$

אז $N(\mathfrak{a} + \mathfrak{b}) = N\mathfrak{a} \cdot N\mathfrak{b}$. בפרט, אם $\mathfrak{p} \in \mathbb{P}$ אז $N\mathfrak{p} = |F_\mathfrak{p}|$. ∎

הגדרה 25.6: **פונקצית זיתא של** F/K היא הפונקצי המרוכבת המוגדרת על ידי

$$\zeta(s) = \zeta_{F/K}(s) = \sum_{\mathfrak{a}\geq 0} \frac{1}{(N\mathfrak{a})^s} = \sum_{\mathfrak{a}\geq 0} q^{-s\deg\mathfrak{a}}, \qquad s\in\mathbb{C} \quad (2)$$
∎

עבור איזה s הטור מתכנס (בהחלט)?

אם נגדיר $t=q^{-s}$ אז $\zeta(s)=Z(t)$, (נקרא ל־$Z(t)$ **פונקצית־זי**) באשר

$$Z(t) = \sum_{\mathfrak{a}\geq 0} t^{\deg\mathfrak{a}} = \sum_{n=0}^{\infty} A_n t^n. \quad (3)$$

משפט 25.7: *הטור* (3) *מתכנס עבור* $|t|<q^{-1}$ *(ולכן* (2) *עבור* $\operatorname{Re}s>1$*). ביתר דיוק, עבור* t *כזה*

(א) אם $g=0$ אז $Z(t)=\frac{1}{q-1}\left(\frac{q}{1-(qt)^\partial}-\frac{1}{1-t^\partial}\right)\in\mathbb{Q}(t)$.

(ב) אם $g\geq 1$ אז $Z(t)=\frac{1}{q-1}\big(F(t)+hG(t)\big)$, באשר

$$F(t) = \sum_{\substack{C\in\mathcal{C}\\ 0\leq\deg C\leq 2g-2}} q^{\dim C}t^{\deg C}\in\mathbb{Q}[t],$$

$$G(t) = \frac{q^{1-g}(qt)^{2g-2+\partial}}{1-(qt)^\partial} - \frac{1}{1-t^\partial}\in\mathbb{Q}(t).$$

הוכחה: תחילה נשים לב ש־$q^{-s}=q^{-\operatorname{Re}s-i\operatorname{Im}s}=q^{-\operatorname{Re}s}e^{i(-\ln q)(\operatorname{Im}s)}$, לכן $|q^{-s}|=q^{-\operatorname{Re}s}$, ומכאן

$$\operatorname{Re}s>1 \Leftrightarrow -\operatorname{Re}s<-1 \Leftrightarrow |q^{-s}|<q^{-1}.$$

(א) לפי תרגיל 16.4, כל מחלק בעל מעלה 0 הוא ראשי, לכן $h=|\mathcal{C}_0|=1$. לפי מסקנה 25.4(ב)

$$\sum_{n=0}^{\infty}A_nt^n = \sum_{m=0}^{\infty}A_{\partial m}t^{\partial m} = \sum_{m=0}^{\infty}\frac{q^{\partial m+1}-1}{q-1}t^{\partial m} =$$
$$= \frac{1}{q-1}\Big(q\sum_{m=0}^{\infty}(qt)^{\partial m}-\sum_{m=0}^{\infty}t^{\partial m}\Big) = \frac{1}{q-1}\Big(\frac{q}{1-(qt)^\partial}-\frac{1}{1-t^\partial}\Big).$$

(ב) לפי למה 25.3

$$\sum_{n=0}^{\infty}A_nt^n = \sum_{n=0}^{\infty}\sum_{C\in\mathcal{C}_n}\frac{q^{\dim C}-1}{q-1}t^n =$$
$$= \frac{1}{q-1}\Big(\sum_{n=0}^{2g-2}\sum_{C\in\mathcal{C}_n}q^{\dim C}t^n + \sum_{n>2g-2}\sum_{C\in\mathcal{C}_n}q^{n+1-g}t^n - \sum_{n=0}^{\infty}\sum_{C\in\mathcal{C}_n}t^n\Big)$$
$$= \frac{1}{q-1}\big(F(t)+hG(t)\big)$$

באשר

$$F(t) = \sum_{n=0}^{2g-2}\Big(\sum_{C\in\mathcal{C}_n}q^{\dim C}\Big)t^n = \sum_{\substack{C\in\mathcal{C}\\ 0\leq\deg C\leq 2g-2}} q^{\dim C}t^{\deg C}$$

$$G(t) = \sum_{n>2g-2}\frac{|\mathcal{C}_n|}{h}q^{n+1-g}t^n - \sum_{n=0}^{\infty}\frac{|\mathcal{C}_n|}{h}t^n = q^{1-g}\sum_{\substack{n=2g-2+\partial\\ \partial|n}}^{\infty}(qt)^n - \sum_{\substack{n=0\\ \partial|n}}^{\infty}t^n$$

שני הסכומים האחרונים הם טורים גיאומטריים שאיבריהם הראשונים הם $1, (qt)^{2g-2+\partial}$ ומנותיהם $t^{\partial}, (qt)^{\partial}$, בהתאמה. לכן $G(t)$ מהצורה המבוקשת. ∎

מסקנה 25.8: *נוסחה (3) מגדירה $Z(t)$ עבור $|t| < q^{-1}$. פונקציה זו ניתנת להרחבה לפונקציה רציונלית על $\mathbb{C}$. הקטבים היחידים שלה הם בנקודות $t^{\partial} = 1$ ו־$t^{\partial} = q^{-\partial}$, והם פשוטים. טור (2) מתכנס עבור $\operatorname{Re} s > 1$, אך על ידי ההצבה $t = q^{-s}$ נוכל להמשיך אותו לפונקציה הולומורפית על כל המישור, פרט לנקודות על הישרים $\operatorname{Re} s = 0$ ו־$\operatorname{Re} s = 1$.*

משפט 25.9: *עבור $\operatorname{Re} s > 1$ ועבור $|t| < q^{-1}$ אפשר להציג את $\zeta(s)$ ואת $Z(t)$ על ידי המכפלות מתכנסות בהחלט*

$$\zeta(s) = \prod_{\mathfrak{p}\in\mathbb{P}} \frac{1}{1-(N\mathfrak{p})^{-s}}, \qquad Z(t) = \prod_{\mathfrak{p}\in\mathbb{P}} \frac{1}{1-t^{\deg \mathfrak{p}}}.$$

הוכחה: הנוסחה הימנית נובעת מהשמאלית על ידי ההצבה $t = q^{-s}$, כי $N\mathfrak{p} = q^{\deg \mathfrak{p}}$. נוכיח את הנוסחה השמאלית. אגף ימין שלה מתכנס בהחלט, כי $\sum_{\mathfrak{p}\in\mathbb{P}} |t^{\deg \mathfrak{p}}| \le \sum_{n=1}^{\infty} A_n t^n < \infty$. נפתח את גורמיו לטורים גיאומטריים ונכפיל אותם:

$$\prod_{\mathfrak{p}\in\mathbb{P}} \frac{1}{1-t^{\deg \mathfrak{p}}} = \prod_{\mathfrak{p}\in\mathbb{P}} \sum_{k(\mathfrak{p})=0}^{\infty} (t^{\deg \mathfrak{p}})^{k(\mathfrak{p})} = \prod_{\mathfrak{p}\in\mathbb{P}} \sum_{k(\mathfrak{p})=0}^{\infty} t^{k(\mathfrak{p})\deg \mathfrak{p}} = \sum_{k} \prod_{\mathfrak{p}\in\mathbb{P}} t^{k(\mathfrak{p})\deg \mathfrak{p}} =$$
$$= \sum_{k} t^{\left(\sum_{\mathfrak{p}} k(\mathfrak{p})\deg \mathfrak{p}\right)} = \sum_{\mathfrak{a}\ge 0} t^{\deg \mathfrak{a}} = Z(t)$$

באשר k עובר על הפונקציות $k\colon \mathbb{P} \to \mathbb{N}\cup\{0\}$ שהינן 0 עבור כמעט כל $\mathfrak{p}$. ∎

מסקנה 25.10: *אם $\operatorname{Re} s > 1$ אז $\zeta(s) \neq 0$. אם $|t| \le q^{-1}$ אז $Z(t) \neq 0$.*

26. פונקצית זיתא והרחבת שדה המקדמים

נשמור את הסימונים וההנחות של הפרק הקודם. מטרת פרק זה היא להוכיח כי $\partial = 1$.

לכל $r \in \mathbb{N}$ יש ל־K הרחבה יחידה ממעלה r; היא גלואה (מעגלית) ותסומן K_r. אז $F_r = K_rF$ הוא שדה פונקציות מעל K_r, הרחבת שדה הקבועים של F/K. הגזע שלה הוא g (משפט 22.11). אם $\mathfrak{a}$ מחלק של F/K אז אפשר לראות אותו כמחלק של F_r/K_r. המעלה והמימד שלו שווים למעלה והמימד של $\mathfrak{a}$ כמחלק של F/K (משפט 22.5(ב) ומשפט 22.10(ב)).

למה 26.1: *יהי $\mathfrak{p}$ מחלק ראשוני של F/K ונסמן $m = \deg\mathfrak{p}$. יהי $\mathfrak{p} = \mathfrak{P}_1 + \cdots + \mathfrak{P}_d$ הפירוק של $\mathfrak{p}$ למחלקים ראשוניים של F_r/K_r. אז $\mathfrak{P}_1, \ldots, \mathfrak{P}_d$ שונים זה מזה, $\deg\mathfrak{P}_i = \frac{m}{\gcd(r,m)}$ לכל i, ו־$d = \gcd(r,m)$.*

הוכחה: נזכיר כי "הפירוק" הנ"ל מתיחס להעתקת הקונורמה $\mathrm{Con}_{F_r/F} : \mathcal{D}(F/K) \to \mathcal{D}(F_r/K_r)$, בעזרתה מזהים את $\mathfrak{p}$ עם תמונתו תחת העתקה זו: $\sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})\mathfrak{P}$. סכום זה הוא "הפירוק" של $\mathfrak{p}$.

לפי למה 23.3, כיון ש־F_r/F הרחבת שדה מקדמים פרידה, $\mathfrak{p}$ אינו מסועף ב־F_r, כלומר, $\mathfrak{P}_1, \ldots, \mathfrak{P}_d$ שונים זה מזה. יהי $1 \le i \le d$. לפי משפט 22.6, $F_{r,\mathfrak{P}_i} = K_rF_{\mathfrak{p}}$. לכן

$$\deg\mathfrak{P}_i = [K_rF_{\mathfrak{p}} : K_r] = [F_{\mathfrak{p}} : (F_{\mathfrak{p}} \cap K_r)] = \frac{[F_{\mathfrak{p}} : K]}{[(F_{\mathfrak{p}} \cap K_r) : K]} = \frac{m}{\gcd(r,m)}$$

כעת, $\deg\mathfrak{p} = d\deg\mathfrak{P}_i$, כלומר, $m = d\frac{m}{\gcd(r,m)}$, ומכאן $d = \gcd(r,m)$. ∎

$$\begin{tikzcd}
 & F_{\mathfrak{p}} \arrow[r, dash] \arrow[d, dash] & K_rF_{\mathfrak{p}} = F_{r,\mathfrak{P}_i} \arrow[d, dash] \\
K \arrow[ur, dash, bend left, "m"] \arrow[r, dash] \arrow[rr, dash, bend right, "r"'] & F_{\mathfrak{p}} \cap K_r \arrow[r, dash] & K_r
\end{tikzcd}$$

משפט 26.2: *תהי Z_r פונקצית זי המתאימה ל־F_r/K_r. אז $Z_r(t^r) = \prod_{\xi^r=1} Z(\xi t)$ לכל $t \in \mathbb{C}$.*

הוכחה: שני האגפים הם פונקציות מירומורפיות, לכן די להוכיח שהן מזדהות עבור $|t| < q^{-1}$. לפי משפט 25.9

$$\prod_{\xi^r=1} Z(\xi t)^{-1} = \prod_{\mathfrak{p}\in\mathbb{P}}\prod_{\xi^r=1}\left(1 - (\xi t)^{\deg\mathfrak{p}}\right), \qquad Z_r(t^r)^{-1} = \prod_{\mathfrak{p}\in\mathbb{P}}\prod_{\mathfrak{P}/\mathfrak{p}}\left(1 - (t^r)^{\deg\mathfrak{P}}\right),$$

לכן די להוכיח את שוויון הגורמים הימניים לכל $\mathfrak{p}$. נקבע $\mathfrak{p}$ ונסמן $m = \deg\mathfrak{p}$, $d = \gcd(r,m)$. אז, לפי למה 26.1, יש d מחלקים ראשוניים $\mathfrak{P}$ מעל $\mathfrak{p}$ והם ממעלה $\deg\mathfrak{P} = \frac{m}{d}$. לכן די להוכיח

$$\left(1 - (t^r)^{\frac{m}{d}}\right)^d = \prod_{\xi^r=1}\left(1 - (\xi t)^m\right),$$

כלומר,

$$(1 - t^{\frac{rm}{d}})^d = \prod_{\xi^r=1}(1 - \xi^m t^m).$$

נסמן $k = \frac{r}{d}$. אם ξ שורש יחידה פרימיטיבי מסדר r אז ξ^m שורש יחידה פרימיטיבי מסדר k. לכן ההעתקה $\xi \mapsto \xi^m$ היא אפימורפיזם מחבורת שרשי היחידה ה־r־ים (איזומורפית ל־$\mathbb{Z}/r\mathbb{Z}$) על חבורת שרשי היחידה ה־k־ים (איזומורפית ל־$\mathbb{Z}/k\mathbb{Z}$). בפרט על כל איבר בחבורה השניה עוברים בדיוק $d = \frac{r}{k}$ איברים שונים מהחבורה הראשונה. לכן אגף ימין של המשוואה הקודמת הוא החזקה ה־d־ית של $\prod_{\eta^k=1}(1-\eta t^m)$. לכן די להוכיח

$$(1) \qquad (1-t^{km}) = \prod_{\eta^k=1}(1-\eta t^m).$$

ואכן, שרשי היחידה ה־k־ים הם כל השרשים השונים של $X^k - 1$, לכן $X^k - 1 = \prod_{\eta^k=1}(X-\eta)$. נציב $X = t^{-m}$ ונכפיל את המשוואה המתקבלת ב־t^{km}, כדי לקבל את (1). ∎

מסקנה 26.3 (F.K. Schmidt): $\partial = 1$.

הוכחה: יהי $r = \partial$. אז $Z(t) = \sum_{m=0}^{\infty} A_{mr}t^{mr}$. לכן אם $\xi \in \mathbb{C}$, $\xi^r = 1$, אז $Z(\xi t) = Z(t)$. לפי המשפט,

$$Z_r(t^r) = Z(t)^r.$$

בנקודה $t = 1$ יש לאגף שמאל קוטב פשוט ולאגף ימין קוטב מסדר r. לכן $\partial = r = 1$. ∎

משפט 26.4: *(א) אם $g = 0$ אז F/K שדה פונקציות רציונליות ו־* $Z(t) = \frac{1}{(1-t)(1-qt)}$.

(ב) אם $g \geq 1$ אז $Z(t) = \frac{1}{q-1}\big(F(t) + hG(t)\big)$, באשר

$$F(t) = \sum_{\substack{C \in \mathcal{C} \\ 0 \leq \deg C \leq 2g-2}} q^{\dim C} t^{\deg C} \in \mathbb{Q}[t],$$

$$G(t) = \frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t}.$$

הוכחה: כיוון ש־$\partial = 1$, יש ל־F/K מחלק בעל מעלה 1. לכן, אם $g = 0$ אז F/K הוא שדה פונקציות רציונליות לפי משפט 16.2. שאר הטענות הן חזרה על משפט 25.7, עם $\partial = 1$. ∎

מסקנה 26.5: $Z(t) = \frac{L(t)}{(1-t)(1-qt)}$, *באשר* $L(t) \in \mathbb{Q}[t]$ *פולינום,* $\deg L \leq 2g$.

משפט 26.6 (המשוואה הפונקציונלית): $Z(t) = q^{g-1}t^{2g-2}Z(\frac{1}{qt})$ *לכל* t.

הוכחה: (א) נניח $g = 0$. אז $Z(t) = \frac{1}{(1-t)(1-qt)}$, לכן

$$q^{-1}t^{-2}Z(\frac{1}{qt}) = \frac{1}{qt}\frac{1}{t}\frac{1}{(1-\frac{1}{qt})(1-\frac{q}{qt})} = \frac{1}{(qt-1)(t-1)} = Z(t).$$

(ב) נניח $g \geq 1$. לפי המשפט הקודם $Z(t) = \frac{1}{q-1}\big(F(t) + hG(t)\big)$, באשר

$$F(t) = \sum_{\substack{C \in \mathcal{C} \\ 0 \leq \deg C \leq 2g-2}} q^{\dim C} t^{\deg C}, \qquad G(t) = \frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t}.$$

לכן די להראות ש־F, G מקיימות את המשוואה הפונקציונלית. ואכן,

$$q^{g-1}t^{2g-2}G(\frac{1}{qt}) = q^{g-1}t^{2g-2}\Big(\frac{q^g\big(\frac{1}{qt}\big)^{2g-1}}{1-\frac{q}{qt}} - \frac{1}{1-\frac{1}{qt}}\Big)$$
$$= \frac{\frac{1}{t}}{1-\frac{1}{t}} - \frac{q^{g-1}t^{2g-2}}{1-\frac{1}{qt}} = \frac{1}{t-1} - \frac{q^g t^{2g-1}}{qt-1} = G(t),$$

$$q^{g-1}t^{2g-2}F(\frac{1}{qt}) = q^{g-1}t^{2g-2}\sum_{\substack{C\in\mathcal{C}\\ 0\leq\deg C\leq 2g-2}} q^{\dim C}(\frac{1}{qt})^{\deg C} =$$
$$= \sum_{\substack{C\in\mathcal{C}\\ 0\leq\deg C\leq 2g-2}} q^{\dim C-\deg C+g-1}t^{2g-2-\deg C} = \sum_{\substack{C\in\mathcal{C}\\ 0\leq\deg C\leq 2g-2}} q^{\dim(W-C)}t^{\deg(W-C)} =$$
$$= F(t).$$

בחישוב האחרון W היא המחלקה הקנונית; לפי משפט רימן־רוך היא מקיימת

$$\deg W = 2g-2, \dim(W-C) = \dim C - \deg C + g - 1.$$

כאשר C עובר על כל המחלקות המקיימות $0 \leq \deg C \leq 2g-2$, גם $W-C$ עובר על אותן המחלקות. לכן בסכום האחרון לעיל אפשר להחליף את $W-C$ ב־C, וכך לקבל את $F(t)$. ∎

27. השערת רימן ומספר המחלקים הראשוניים ממעלה 1

נשמור את הסימון ואת ההנחות של שני הפרקים הקודמים.

נסמן ב־N את מספר המחלקים הראשוניים ממעלה 1 של F/K. נזכור ש־$Z(t) = \sum_n A_n t^n$, באשר $A_n = |\{\mathfrak{b} |\ \deg \mathfrak{b} = n,\ \mathfrak{b} \geq 0\}|$.

תרגיל 27.1: $A_0 = 1$, $A_1 = N$.

הוכחה: מחלק אי שלילי הוא ממעלה:

0 אם ורק אם הוא מחלק האפס;

1 אם ורק אם הוא מחלק ראשוני ממעלה 1. ∎

לפי מסקנה 26.5, $Z(t) = \frac{L(t)}{(1-t)(1-qt)}$, באשר $L[t] \in \mathbb{Q}[t]$ **פולינום**־L, $\deg L \leq 2g$, נאמר

$$L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}.$$

למה 27.2: *(א)* $L(t) = \frac{Z(t)}{Z_0(t)}$, *באשר* $Z_0(t)$ *פונקצית־זי של שדה הפונקציות הרציונליות מעל* K.

(ב) *המשוואה הפונקציונלית:* $L(t) = q^g t^{2g} L(\frac{1}{qt})$.

(ג) $a_{2g-i} = q^{g-i} a_i$ *לכל* $0 \leq i \leq 2g$.

(ד) $a_0 = 1$, $a_1 = N - (q+1)$, $a_{2g-1} = q^{g-1}\big(N-(q+1)\big)$, $a_{2g} = q^g$. *בפרט* $\deg L = 2g$.

(ה) $q^g = \prod_{i=1}^{2g} \omega_i$, $L(t) = \prod_{i=1}^{2g}(1-\omega_i t)$, *באשר* $\omega_1^{-1}, \ldots, \omega_{2g}^{-1} \in \mathbb{C}^\times$ *השרשים של* $L(t)$.

(ו) $N - (q+1) = a_1 = -\sum_{i=1}^{2g} \omega_i$.

(ז) *אפשר לסדר את* $\omega_1, \ldots, \omega_{2g}$ *כך ש־* $\omega_i \omega_{g+i} = q$ *לכל* $1 \leq i \leq g$.

הוכחה: (א) לפי משפט 26.4, $Z_0(t) = \frac{1}{(1-t)(1-qt)}$. מכאן המסקנה.

(ב) לפי המשוואות הפונקציונליות (משפט 26.6) עבור Z, Z_0

$$L(t) = \frac{Z(t)}{Z_0(t)} = \frac{q^{g-1}t^{2g-2}Z(\frac{1}{qt})}{q^{-1}t^{-2}Z_0(\frac{1}{qt})} = q^g t^{2g} L(\frac{1}{qt}).$$

(ג) את המשוואה הקודמת אפשר לרשום כך:

$$\sum_{i=0}^{2g} a_i t^i = q^g t^{2g}\Big(\sum_{j=0}^{2g} a_j (qt)^{-j}\Big) = \sum_{j=0}^{2g} a_j q^{g-j} t^{2g-j} = \sum_{i=0}^{2g} a_{2g-i} q^{i-g} t^i.$$

השוואת המקדמים של שני האגפים נותנת את קשרים המבוקשים.

(ד) מתוך $L(t) = \frac{Z(t)}{Z_0(t)}$ נקבל

$$L(t) = (1-t)(1-qt)Z(t) = (1-t)(1-qt)(A_0 + A_1 t + \ldots) =$$
$$= A_0 + (A_1 - A_0 - qA_0)t + \ldots = 1 + \big(N-(q+1)\big)t + \ldots$$

מכאן נקבל את a_0, a_1. האיברים הנוספים מתקבלים מהם לפי (ג).

(ה) השורשים של $L(t) = \sum_{i=0}^{2g} a_i t^i$ שונים מאפס, כי $a_0 \neq 0$. אם נכתוב אותם כ־$\{\omega_i^{-1}\}_{i=1}^{2g}$ אז

$$\prod_{i=1}^{2g} \omega_i = \frac{a_{2g}}{a_0} = a_{2g} = q^g, \tag{1}$$

לכן $L(t) = a_{2g} \prod_{i=1}^{2g}(t - \omega_i^{-1}) = \prod_{i=1}^{2g} \omega_i \cdot \prod_{i=1}^{2g}(t - \omega_i^{-1}) = \prod_{i=1}^{2g}(1 - \omega_i t)$.

(ו) השוויון השמאלי הוא (ד). השוויון הימני נובע מההצגה $L(t) = \prod_{i=1}^{2g}(1 - \omega_i t)$ בסעיף (ה).

(ז) לפי (1), $q^g = \prod_{i=1}^{2g} \omega_i$. לכן לפי (ב)

$$L(t) = q^g t^{2g} L(\frac{1}{qt}) = \frac{(qt)^{2g}}{\prod_{i=1}^{2g} \omega_i} \prod_{i=1}^{2g} (1 - \frac{\omega_i}{qt}) = \prod_{i=1}^{2g} (\frac{qt}{\omega_i} - 1) = \prod_{i=1}^{2g} (1 - \frac{qt}{\omega_i}).$$

לכן הסדרה $(\frac{q}{\omega_i})_{i=1}^{2g}$ היא תמורה של הסדרה $(\omega_i)_{i=1}^{2g}$. לכן, לאחר סידור מחדש, $(\omega_i)_{i=1}^{2g}$ הם

$$\omega_1, \frac{q}{\omega_1}, \ldots, \omega_k, \frac{q}{\omega_k}, \overbrace{q^{\frac{1}{2}}, \ldots, q^{\frac{1}{2}}}^{m}, \overbrace{-q^{\frac{1}{2}}, \ldots, -q^{\frac{1}{2}}}^{n}$$

באשר $2k + m + n = 2g$. לפי (ה), $q^g = q^k \cdot q^{\frac{m}{2}} (-1)^n q^{\frac{n}{2}} = (-1)^n q^g$. לכן n זוגי. מתוך $2k + m + n = 2g$ גם m זוגי. מכאן הטענה ברורה. ∎

משפט 27.3 (השערת רימן לשדות פונקציות): *(א) כל האפסים של $\zeta(s)$ נמצאים על הישר $s = \frac{1}{2}$.*

(ב) כל האפסים של $Z(t)$ נמצאים על המעגל $|t| = q^{\frac{-1}{2}}$.

(ג) אם $L(t) = \prod_{i=1}^{2g}(1 - \omega_i t)$ אז $|\omega_i| = \sqrt{q}$ לכל i.

תנאים (א), (ב), (ג) שקולים זה לזה, כי $Z(t) = \zeta(s)$, אם $t = q^{-s}$, ו־$Z(t) = 0$ אם ורק אם $L(t) = 0$.

את המשפט נוכיח מאוחר יותר. כרגע נסיק ממנו מסקנה חשובה.

משפט 27.4: $|N - (q+1)| \leq 2g\sqrt{q}$.

הוכחה: לפי למה 27.2(ו), $N - (q+1) = -\sum_{i=1}^{2g} \omega_i$. לכן

$$|N - (q+1)| \leq \sum_{i=1}^{2g} |\omega_i| \leq 2g\sqrt{q}. \quad \blacksquare$$

ניסוח אחר של אותה ההשערה, במונחים של גיאומטריה אלגברית:

משפט 27.5: *יהי Γ עקום פרויקטיבי אי פריק לחלוטין המוגדר מעל K. יהי g הגזע שלו (הגזע של שדה הפונקציות שלו) ויהי N מספר הנקודות הרציונליות־K שלו. אז $|N - (q+1)| \leq 2g\sqrt{q}$.*

הוכחה: הנקודות הרציונליות־K של Γ מתאימות למחלקים הראשוניים ממעלה 1 של שדה הפונקציות של Γ.

(אם העקום נתון על ידי משוואה פולינומיאלית $f(X,Y)=0$, אז שדה המנות של החוג $K[x,y]=K[X,Y]/(f(X,Y))$ הוא שדה פונקציות אלגבריות במשתנה אחד מעל K. זה ש־f אי פריק לחלוטין –כלומר, אי פריק מעל הסגור האלגברי של K– מבטיח ש־K סגור אלגברית ב־$K(x,y)$.) ∎

למשפט זה קיימת הכללה:

משפט 27.6 (Lang-Weil): *תהי V יריעה אי פריקה לחלוטין ממימד r וממעלה d המוגדרת מעל K, מוכלת במרחב הפרויקטיבי ממימד n. יהי N מספר הנקודות הרציונליות־K שלה. אז קיים $A>0$ (התלוי רק ב־r,n,d) כך ש־ אז* $|N-q^r|\le(d-1)(d-2)q^{r-\frac{1}{2}}+Aq^{r-1}$.

28. תנאים שקולים להשערת רימן

נשמור את הסימון ואת ההנחות של שני הפרקים הקודמים. לכל $r \in \mathbb{N}$ יהי N_r מספר המחלקים הראשוניים ממעלה 1 של ההרחבה F_r/K_r. יהי L_r פולינום־L המתאים ל־F_r/K_r. (אז $N = N_1, L = L_1$.)

משפט 28.1: *יהי $r \in \mathbb{N}$. אז $L_r(t) = \prod_{i=1}^{2g}(1-\omega_i^r t)$. השערת רימן עבור F/K נכונה אם ורק אם השערת רימן עבור F_r/K_r נכונה.*

הוכחה: לפי למה 27.2(א), $L_r(t) = \frac{Z_r(t)}{Z_{0r}(t)}$, באשר Z_{0r}, Z_r פונקציות־זי של F_r/K_r ושל שדה הפונקציות הרציונליות מעל K_r, בהתאמה. לפי משפט 26.2, $Z_r(t^r) = \prod_{\xi^r=1} Z(\xi t)$. לכן

$$L_r(t^r) = \frac{Z_r(t^r)}{Z_{0r}(t^r)} = \frac{\prod_{\xi^r=1} Z(\xi t)}{\prod_{\xi^r=1} Z_0(\xi t)} = \prod_{\xi^r=1} L(\xi t) = \prod_{\xi^r=1}\prod_{i=1}^{2g}(1-\omega_i \xi t) = \prod_{i=1}^{2g}(1-\omega_i^r t^r),$$

(השוויון הימני נובע מהזהות $X^r - 1 = \prod_{\xi^r=1}(X-\xi)$, בה מציבים $X = \omega_i^{-1}t^{-1}$ ואחר כך מכפילים ב־$\omega_i^r t^r$) לכן $L_r(t) = \prod_{i=1}^{2g}(1-\omega_i^r t)$. ברור ש־

$$|\omega_i| = \sqrt{q} \Leftrightarrow |\omega_i^r| = \sqrt{q^r}, \qquad i = 1, \ldots, 2g.$$

שני האגפים של השקילות מבטאים את השערות רימן עבור שתי ההרחבות, לכן ההשערות שקולות. ∎

משפט 28.2: *אם קיים c כך שלכל $r \in \mathbb{N}$*

$$|N_r - (q^r+1)| \le c q^{\frac{r}{2}}, \tag{2}$$

אז השערת רימן עבור F/K נכונה.

הוכחה: תהי $M(t) = \sum_{i=1}^{2g} \frac{-1}{1-\omega_i t} \in \mathbb{C}(t)$. זוהי פונקציה הולומורפית בסביבה של 0; יהי R רדיוס ההתכנסות שלה. הנקודות הסינגולריות (קטבים) היחידות שלה הן $\{\omega_i^{-1}\}_{i=1}^{2g}$, לכן

$$R = \min_i |\omega^{-1}|. \tag{3}$$

מצד שני, פיתוח טיילור של $M(t)$ סביב 0, לפי למה 27.2(ו), הוא

$$M(t) = \sum_{r=0}^{\infty}\Big(-\sum_{i=1}^{2g}\omega_i^r)\Big)t^r = \sum_{r=0}^{\infty}\big(N_r - (q^r+1)\big)t^r,$$

ולפי ההנחה (2) טור זה מתכנס עבור $|t| < q^{-\frac{1}{2}}$. מכאן $R \ge q^{-\frac{1}{2}}$. לכן לפי (3), $|\omega_i^{-1}| \ge R \ge q^{-\frac{1}{2}}$, כלומר, $|\omega_i| \le \sqrt{q}$ לכל i. אבל $\prod_i \omega_i = q^g$. לכן $|\omega_i| = \sqrt{q}$ לכל i. ∎

כדי להוכיח את השערת רימן, נשתמש בגרסה (2) עבור הרחבת שדות מקדמים מתאימה. בנוסף לכך נכליל את ההשערה.

הערה 28.3: אם M שדה בעל אפיון $p > 0$ ו־q חזקה של p אז $x \mapsto x^q$ הוא שיכון (מונומורפיזם) של שדות $M \to M$. הוא הזהות על M אם ורק אם M תת שדה של השדה K בן q איברים. אם L/K הרחבה סופית (או אפילו אלגברית), אז $x \mapsto x^q$ הוא אוטומורפיזם של L (נקרא אוטומורפיזם Frobenius). ∎

הגדרה 28.4: יהי σ אוטומורפיזם של F מעל K. לכל מחלק ראשוני $\mathfrak{p}$ של F/K נבחר אתר $\varphi_{\mathfrak{p}} \colon F \to F_{\mathfrak{p}} \cup \{\infty\}$, שהינו הזהות על K, אשר מייצג את $\mathfrak{p}$. נסמן

$$H^{(\sigma)}(F) = \left\{\mathfrak{p} \in \mathbb{P} \mid \varphi_{\mathfrak{p}}(x) = \varphi_{\mathfrak{p}}\left((\sigma x)^q\right) = \left(\varphi_{\mathfrak{p}}(\sigma x)\right)^q \text{ לכל } x \in F\right\}$$

$$N^{(\sigma)}(F) = \sum_{\mathfrak{p} \in H^{(\sigma)}(F)} \deg \mathfrak{p}.$$

את התנאי "$\varphi_{\mathfrak{p}}(x) = \left(\varphi_{\mathfrak{p}}(\sigma x)\right)^q$ לכל $x \in F$" אפשר לרשום גם כ־$\varphi_{\mathfrak{p}} = \mathrm{Frob} \circ \varphi_{\mathfrak{p}} \circ \sigma$, באשר $\mathrm{Frob} \in \mathrm{Aut}(\tilde{K}/K)$ מוגדר על ידי $x \mapsto x^q$. ∎

$$\begin{tikzcd} F \arrow[r, "\varphi_{\mathfrak{p}}"] \arrow[d, "\sigma"] & K \cup \{\infty\} \arrow[d, "\mathrm{Frob}"] \\ F \arrow[r, "\varphi_{\mathfrak{p}}"] & K \cup \{\infty\} \end{tikzcd}$$

הערה 28.5: אם $\sigma = \mathrm{id}$ אז

$$H^{(\sigma)}(F) = \{\mathfrak{p} \in \mathbb{P} \mid F_{\mathfrak{p}} = K\}$$

$$N^{(\sigma)}(F) = \sum_{\mathfrak{p} \in H^{(\sigma)}(F)} 1 = N.$$ ∎

תרגיל 28.6: *הראה שההגדרה של $N^{(\sigma)}(F)$ אינה תלויה בבחירת המייצג $\varphi_{\mathfrak{p}}$ של $\mathfrak{p}$.*

29. חסם מלעיל

נשמור את הסימון ואת ההנחות של הפרקים הקודמים.

משפט 29.1: *יהי σ אוטומורפיזם של F מעל K. נניח*

(א) $\sqrt{q} \in \mathbb{N}$.

(ב) $q > (g+1)^4$

(ג) *ל־F/K יש מחלק ראשוני $\mathfrak{o}$ ממעלה* 1.

אז

$$N^{(\sigma)}(F) - (q+1) < (2g+1)\sqrt{q}. \tag{1}$$

הוכחה: נסמן

$$q' = \sqrt{q}, \qquad m = q'-1, \qquad n = q'+2g, \qquad r = m + q'n. \tag{2}$$

אז

$$r = (q'-1) + q'(q'+2g) = (2g+1)q' + (q')^2 - 1 = (2g+1)\sqrt{q} + q - 1.$$

לכן את (1) אפשר לרשום כך (מחליפים "$<$" ב־"$\leq$"):

$$N^{(\sigma)}(F) - 1 \leq r. \tag{3}$$

תהי v הערכה מתאימה למחלק הראשוני $\mathfrak{o}$. קיימת סדרה עולה של מרחבים וקטוריים מעל K

$$0 = \mathcal{L}((-1)0) \subseteq K = \mathcal{L}(0) \subseteq \mathcal{L}(\mathfrak{o}) \subseteq \mathcal{L}(2\mathfrak{o}) \subseteq \mathcal{L}(3\mathfrak{o}) \subseteq \ldots$$

אם $\mathcal{L}\big((i-1)\mathfrak{o}\big) \subsetneqq \mathcal{L}\big(i\mathfrak{o}\big)$, נבחר $u_i \in \mathcal{L}\big(i\mathfrak{o}\big) \smallsetminus \mathcal{L}\big((i-1)\mathfrak{o}\big)$. אז

$$(u_i)_\infty = i\mathfrak{o} \tag{4}$$

ובפרט $v(u_i) = -i$. עבור $k \in \mathbb{N}$ נסמן $I_k = \big\{0 \leq i \leq k |\ \mathcal{L}\big((i-1)\mathfrak{o}\big) \subsetneqq \mathcal{L}\big(i\mathfrak{o}\big)\big\}$. אם $i \in I_k$ אז, לפי תרגיל 7.9, $\dim_K \mathcal{L}\big(i\mathfrak{o}\big) - \dim_K \mathcal{L}\big((i-1)\mathfrak{o}\big) = 1$. לכן $\{u_i |\ i \in I_k\}$ בסיס של $\mathcal{L}(k\mathfrak{o})$.

טענה 1: *$\{u_i |\ i \in I_m\}$ בלתי תלויה לינארית מעל $(F)^{q'}$.* אכן, אחרת יש $\emptyset \neq I \subseteq I_m$ ולכל $i \in I$ יש $y_i \in F^\times$ כך ש־$\sum_{i \in I} (y_i)^{q'} u_i = 0$. לא יתכן כי $|I| = 1$, כי $u_i \neq 0$ לכל i. לפי טענה 1.10(ה) יש $i, j \in I$ שונים כך ש־$v\big((y_i)^{q'} u_i\big) = v\big((y_j)^{q'} u_j\big)$, כלומר, $q'v(y_i) - i = q'v(y_j) - j$. מכאן $i \equiv j \mod q'$, סתירה, כי $0 \leq i, j \leq m < q'$.

טענה 2: $\{u_iu_j^{q'} \mid i\in I_m,\ j\in I_n\}$ *בלתי תלויה לינארית מעל K.* אכן, $F \subseteq \{u_j|\ j\in I_n\}$ בלתי תלויה לינארית מעל K, לכן $F^{q'} \subseteq \{u_j^{q'} \mid j\in I_n\}$ בלתי תלויה לינארית מעל $K^{q'} = K$. לכן המסקנה נובעת לפי טענה 1.

$$K = K^{q'} \text{------} F^{q'} \text{------} F$$

נגדיר

$$\mathcal{L} := \mathrm{Sp}_K(u_iu_j^{q'} \mid i\in I_m,\ j\in I_n), \qquad \mathcal{L}' := \mathcal{L}\big(mq'(\sigma\mathfrak{o}) + n\mathfrak{o}\big).$$

אז $\dim_K \mathcal{L} = |I_m|\cdot|I_n| = \dim(m\mathfrak{o})\cdot\dim(n\mathfrak{o})$. לכן לפי משפט רימן־רוך

$$\dim_K \mathcal{L} \geq (m-g+1)(n-g+1) = (q'-g)(q'+g+1) = q-g^2+q'-g \tag{5}$$

כיוון ש־

$$\deg\big(mq'(\sigma\mathfrak{o}) + n\mathfrak{o}\big) = mq'+n = (q'-1)q' + (q'+2g) = q+2g > 2g-2,$$

לפי רימן־רוך

$$\dim_K \mathcal{L}\big(mq'(\sigma\mathfrak{o}) + n\mathfrak{o}\big) = (q+2g)+1-g = q+g+1$$

לפי (ב), $q' > (g+1)^2 = g^2+2g+1$, לכן $q'-g^2-g > g+1$, ומכאן

$$\dim_K \mathcal{L} > \dim_K \mathcal{L}'. \tag{6}$$

טענה 3: $\{(\sigma u_i)^{q'}u_j|\ i\in I_m,\ j\in I_n\} \subseteq \mathcal{L}'$. אכן, $u_i \in \mathcal{L}(m\mathfrak{o})$, כלומר, $(u_i)+m\mathfrak{o} \geq 0$. מכאן $(\sigma u_i) + m(\sigma\mathfrak{o}) \geq 0$ ולכן $\big((\sigma u_i)^{q'}\big) + mq'(\sigma\mathfrak{o}) \geq 0$. מצד שני $u_j \in \mathcal{L}(n\mathfrak{o})$, כלומר, $(u_j)+n\mathfrak{o} \geq 0$. מכאן

$$\big((\sigma u_i)^{q'}u_j\big) + mq'(\sigma\mathfrak{o}) + n\mathfrak{o} = \big((\sigma u_i)^{q'}\big) + mq'(\sigma\mathfrak{o}) + \big(u_j\big) + n\mathfrak{o} \geq 0.$$

האיזומורפיזם $x\mapsto x^{q'}$ מעתיק את $\mathcal{L}$ על המרחב הוקטורי $\mathcal{L}^{q'}$ מעל $K^{q'}=K$. האיזומורפיזם מעתיק בסיס לבסיס. נגדיר העתקה לינארית־K $T\colon \mathcal{L}^{q'} \to \mathcal{L}'$ על ידי $(u_iu_j^{q'})^{q'} \mapsto (\sigma u_i)^{q'}u_j$. לפי (6), $\operatorname{Ker} T \neq 0$. לכן יש $a_{ij}\in K$ כך ש־

$$u := \sum_{i\in I_m}\sum_{j\in I_n} a_{ij}u_iu_j^{q'} \neq 0, \qquad \sum_{i\in I_m}\sum_{j\in I_n} a_{ij}^{q'}(\sigma u_i)^{q'}u_j = 0.$$

אם $i\in I_m$ ו־$j\in I_n$ אז $(u_i)\in\mathcal{L}(m\mathfrak{o}), (u_j^{q'})\in\mathcal{L}(nq'\mathfrak{o})$ לכן $u_iu_j^{q'} \in \mathcal{L}\big((m+nq')\mathfrak{o}\big) = \mathcal{L}(r\mathfrak{o})$. מכאן $u\in\mathcal{L}(r\mathfrak{o})$. בפרט

$$\deg(u)_\infty \leq r.$$

טענה 4: *יהי* $\mathfrak{p} \neq \mathfrak{o} \in H^{(\sigma)}(F)$. אז $\varphi_{\mathfrak{p}}(u) = 0$. אכן, לפי (4), $\varphi_{\mathfrak{p}}(u_i) \neq \infty$ לכל i. מכאן

$$\varphi_{\mathfrak{p}}(u) = \sum_{i\in I_m}\sum_{j\in I_n} a_{ij}\varphi_{\mathfrak{p}}(u_i)\varphi_{\mathfrak{p}}(u_j)^{q'} = \sum_{i\in I_m}\sum_{j\in I_n} a_{ij}^{q}\varphi_{\mathfrak{p}}(\sigma u_i)^{q}\varphi_{\mathfrak{p}}(u_j)^{q'} =$$
$$= \Big(\sum_{i\in I_m}\sum_{j\in I_n} a_{ij}^{q'}\varphi_{\mathfrak{p}}(\sigma u_i)^{q'}\varphi_{\mathfrak{p}}(u_j)\Big)^{q'} = \varphi_{\mathfrak{p}}\Big(\sum_{i\in I_m}\sum_{j\in I_n} a_{ij}^{q'}(\sigma u_i)^{q'}u_j\Big)^{q'} = 0$$

מהטענה נובע כי $\sum_{\substack{\mathfrak{p}\in H^{(\sigma)}(F)\\ \mathfrak{p}\neq\mathfrak{o}}} \mathfrak{p} \leq (u)_0$, לכן

$$.N^{(\sigma)}(F) - 1 \leq \sum_{\substack{\mathfrak{p}\in H^{(\sigma)}(F)\\ \mathfrak{p}\neq\mathfrak{o}}} \deg\mathfrak{p} \leq \deg(u)_0 = \deg(u)_\infty \leq r \qquad \blacksquare$$

30. תרגילי הכנה

תרגיל 30.1: *יהי E/K שדה פונקציות ותהי F/L הרחבה נורמלית שלו. יהי φ אתר של E טריביאלי על K, ויהיו ψ, ψ' שני אתרים של F טריביאליים על L שמרחיבים את φ ושדות השאריות שלהם מוכלים ב־$\tilde{K}$. אז יש $\sigma \in \mathrm{Aut}(F/E)$ כך ש־$\psi' = \psi \circ \sigma$.*

הוכחה: יהי $\mathfrak{p}$ המחלק הראשוני של E/K שמתאים ל־φ ויהיו $\mathfrak{P}, \mathfrak{P}'$ המחלקים הראשוניים של F/L שמתאימים ל־ψ, ψ', בהתאמה. אז $\mathfrak{P}, \mathfrak{P}'$ מעל $\mathfrak{p}$, לכן לפי משפט 20.4 יש $\sigma' \in \mathrm{Aut}(F/E)$ כך ש־ $\sigma'\mathfrak{P} = \mathfrak{P}'$. נחליף את ψ ב־$\psi \circ \sigma'$ ואת $\mathfrak{P}$ ב־$\sigma'\mathfrak{P}$ כדי להניח ש־$\mathfrak{P}' = \mathfrak{P}$. לכן ψ, ψ' אתרים שקולים. בפרט יש להם אותו חוג הערכה $\mathcal{O}$.

יהיו $F_\mathfrak{P}, F'_\mathfrak{P}$ שדות השאריות של ψ, ψ', ויהי $E_\mathfrak{p}$ שדה השאריות של φ. בהתאמה. לפי תרגיל 1.21, יש איזומורפיזם $\tau\colon F_\mathfrak{P} \to F'_\mathfrak{P}$ כך ש־$\psi' = \tau \circ \psi$. בפרט $\varphi = \tau|_{E_\mathfrak{p}} \circ \varphi$, לכן $\tau|_{E_\mathfrak{p}} = \mathrm{id}$. אבל לפי משפט 20.7(א), $F_\mathfrak{P}/E_\mathfrak{p}$ נורמלית, לכן $F'_\mathfrak{P} = \tau(F_\mathfrak{P}) = F_\mathfrak{P}$.

לכן $\tau \in \mathrm{Aut}(F_\mathfrak{P}/E_\mathfrak{p})$. בלי הגבלת הכלליות $\psi\colon \mathcal{O} \to F_\mathfrak{P}$ היא העתקת המנה מודולו האידאל המרבי של $\mathcal{O}$. לפי משפט 20.7(ב), יש $\sigma \in D(\mathfrak{P}) \le \mathrm{Aut}(F/E)$ כך ש־$\tau = \bar{\sigma}$, כלומר, $\psi \circ \sigma = \tau \circ \psi$. מכאן $\psi \circ \sigma = \psi'$. ∎

תרגיל 30.2: *יהי F/K שדה פונקציות ויהי $K \subsetneqq E \subseteq F$ שדה ביניים. אז E/K שדה פונקציות.*

הוכחה: השדה K סגור אלגברית בתוך F ולכן גם בתוך E. כיוון ש־$E \neq K$, קיים $x \in E \smallsetminus K$. בפרט $x \in F \smallsetminus K$, לכן x טרנסצנדנטי מעל K ו־$F/K(x)$ סופית. לכן גם $E/K(x)$ סופית. בפרט E/K נוצרת סופית ו־$\mathrm{tr.\,deg}E/K = 1$. ∎

תרגיל 30.3: *יהי F שדה פונקציות מעל שדה משוכלל K (כל הרחבה סופית של K פרידה). אז יש $x \in F$ כך ש־$F/K(x)$ סופית פרידה.*

הוכחה: אפשר לכתוב $F = K(x_1, \ldots, x_n)$. בלי הגבלת הכלליות $x_i \notin K$ לכל i. אז x_i טרנסצנדנטי מעל K ו־$F/K(x_i)$ סופית לכל i; נראה שיש i כך שהיא פרידה. בלי הגבלת הכלליות $p := \mathrm{char}\ K > 0$.

אם $n = 1$, הטענה ברורה. נניח $n = 2$. אז x_1, x_2 תלויים אלגברית מעל K. לכן יש $0 \neq f \in K[X_1, X_2]$ כך ש־$f(x_1, x_2) = 0$. נבחר f כזה ממעלה מזערית. אז f אי פריק ב־$K[X_1, X_2]$ ולכן ב־$K[X_1][X_2]$. לפי הלמה של גאוס הוא גם אי פריק ב־$K(X_1)[X_2]$. כיוון ש־$K(X_1) \cong_K K(x_1)$, הפולינום $g(X_2) = f(x_1, X_2) \in K(x_1)[X_2]$ אי פריק מעל $K(x_1)$. באותו אופן $f(X_1, x_2)$ אי פריק מעל $K(x_2)$.

לפי ההנחה, כל $a \in K$ הוא חזקה p־ית של איבר ב־K. לא יתכן ששני המשתנים X_1, X_2 מופיעים בכל המונומים של f (בעלי מקדם שונה מאפס) בחזקה שהיא כפולה של p, כי אז f היה חזקה p־ית של פולינום מעל K, בסתירה למזעריות המעלה. בלי הגבלת הכלליות X_2 אינו מופיע בכל המונומים של f בחזקה שהיא כפולה של p. אז

X_2 אינו מופיע בכל המונומים של g בחזקה שהיא כפולה של p. מכאן $g' \neq 0$; כיוון ש־g אי פריק ו־$g(x_2) = 0$, x_2 פריד מעל $K(x_1)$. לכן $K(x_1, x_2)/K(x_1)$ הרחבה פרידה.

אם $n > 2$, הטענה נובעת באינדוקציה על n. אכן, לפי הפסקה הקודמת, בלי הגבלת הכלליות x_n פריד מעל $K(x_1)$. בפרט $F/K(x_1, \ldots, x_{n-1})$ פרידה. לפי הנחת האינדוקציה יש $1 \leq i \leq n-1$ כך ש־$K(x_1, \ldots, x_{n-1})/K(x_i)$ פרידה. אז $F/K(x_i)$ פרידה. ∎

תרגיל 30.4: *יהי F/K שדה פונקציות ויהי $K \subseteq E \subseteq F$ שדה ביניים. תהי L/K הרחבה פרידה סופית. (כל השדות מוכלים בשדה משותף.) אז $F \cap (EL) = E$.*

הוכחה: יהי $n = [L : K]$, יהי α איבר פרימיטיבי עבור L/K ויהי f הפולינום האי פריק המתוקן של α מעל K.

$$\begin{tikzcd}
 & F \arrow[r, dash] \arrow[d, dash] & FL \arrow[d, dash] \\
E \arrow[r, dash] & F \cap (EL) \arrow[r, dash] & EL
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
F \arrow[r, dash] \arrow[d, dash] & FL = F(\alpha) \arrow[d, dash] \\
E \arrow[r, dash] \arrow[d, dash] & EL = E(\alpha) \arrow[d, dash] \\
K \arrow[r, dash] & L = K(\alpha)
\end{tikzcd}$$

לפי תרגיל 6.7, f נשאר אי פריק מעל F, ולכן, בפרט, מעל E. לכן $[FL : F] = [EL : E] = [L : K] = \deg f$. אבל $[EL : E] \leq [EL : F \cap (EL)] \leq [FL : F]$. מכאן ששני האי שוויונים הם שוויונים ולכן $F \cap (EL) = E$. ∎

תרגיל 30.5: *יהי F/K שדה פונקציות ויהי $\sigma \in \mathrm{Aut}(F/K)$. תהי L/K הרחבה פרידה סופית. אז ניתן להרחיב את σ לאוטומורפיזם יחיד $\hat{\sigma}$ של FL/L.*

הוכחה: יהי $n = [L : K]$, יהי α איבר פרימיטיבי עבור L/K ויהי f הפולינום האי פריק המתוקן של α מעל K. לפי תרגיל 6.7, f נשאר אי פריק מעל F. לכן לכל $z \in FL$ הצגה יחידה

$$z = \sum_{i=0}^{n-1} a_i \alpha^i, \qquad a_i \in F. \tag{1}$$

אם $\hat{\sigma} \in \mathrm{Aut}(FL/L)$, מרחיב את σ, אז מתקיים, בהינתן הצגה (1),

$$\hat{\sigma}(z) = \hat{\sigma}\Big(\sum_{i=0}^{n-1} a_i \alpha^i\Big) = \sum_{i=0}^{n-1} \sigma(a_i) \alpha^i. \tag{2}$$

מכאן היחידות. כמו כן מגדירה (2) העתקה $\hat{\sigma}\colon FL \to FL$.

אם $z = \sum_{i=0}^{n-1} a_i \alpha^i \in L$ אז $a_i \in K$ ולכן $\sigma(a_i) = a_i$ ומכאן $\hat{\sigma}(z) = z$. לכן $\hat{\sigma}$ שומרת אברי L. בפרט $\hat{\sigma}(\alpha^k) = \alpha^k$ לכל $k \geq 0$.

קל לראות ש־$\hat{\sigma}$ שומרת חיבור וכפל באברי F. **בהסתמתך על כך**, נראה שהיא שומרת כפל:

$$\hat{\sigma}\Big(\big(\sum_i a_i\alpha^i\big)\big(\sum_j b_j\alpha^j\big)\Big) = \hat{\sigma}\Big(\sum_k\big(\sum_{i+j=k} a_ib_j\big)\alpha^k\Big) = \sum_k\sum_{i+j=k}\hat{\sigma}(a_ib_j\alpha^k) =$$

$$= \sum_k\sum_{i+j=k}\hat{\sigma}(a_ib_j)\hat{\sigma}(\alpha^k) = \sum_k\sum_{i+j=k}\sigma(a_ib_j)\alpha^k$$

$$\hat{\sigma}\big(\sum_i a_i\alpha^i\big)\hat{\sigma}\big(\sum_j b_j\alpha^j\big) = \big(\sum_i\sigma(a_i)\alpha^i\big)\big(\sum_j\sigma(b_j)\alpha^j\big) = \sum_k\sum_{i+j=k}\sigma(a_ib_j)\alpha^k$$

ושני הביטויים שווים זה לזה. ∎

31. חסם מלרע

נחזור אל הסימון וההנחות של הפרקים הקודמים (לפני פרק 30).

למה 31.1: *יהי* $K \subseteq E \subseteq F$ *שדה ביניים כך ש־*F/E *הרחבת גלואה סופית. יהי* $\sigma \in \mathrm{Aut}(F/K)$ *כך ש־*$\sigma(E) = E$*. נסמן* $G = \mathrm{Gal}(F/E)$*. אז*

$$N^{(\sigma)}(E) = \frac{1}{[F:E]} \sum_{\tau \in G} N^{(\tau\sigma)}(F). \tag{1}$$

הוכחה: לפי תרגיל 30.2, גם E/K שדה פונקציות ו־F/K היא הרחבה סופית שלו (עם אותו שדה קבועים). אנו מסמנים גם את הצמצום של σ ל־E ב־σ.

אם $\mathfrak{p}$ מחלק ראשוני של E/K אז לפי השוויון היסודי

$$[F:E] = \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) = \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \frac{\deg \mathfrak{P}}{\deg \mathfrak{p}}.$$

מכאן, לפי הגדרה 28.4,

$$[F:E] \cdot N^{(\sigma)}(E) = [F:E] \sum_{\mathfrak{p} \in H^{(\sigma)}(E)} \deg \mathfrak{p} = \sum_{\mathfrak{p} \in H^{(\sigma)}(E)} \sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) \deg \mathfrak{P},$$

$$\sum_{\tau \in G} N^{(\tau\sigma)}(F) = \sum_{\tau \in G} \sum_{\mathfrak{P} \in H^{(\tau\sigma)}(F)} \deg \mathfrak{P}$$

בשתי הנוסחאות לעיל מסכמים $\deg \mathfrak{P}$ עבור איזשהם $\mathfrak{P}$, עם איזשהם מקדמים; יתקיים שוויון אם בשתי הנוסחאות מופיעים אותם $\mathfrak{P}$־ים וכל אחד עם אותו המקדם.

לכן כדי להוכיח את (1), די להוכיח לכל $\mathfrak{P}/\mathfrak{p}$:

(א) $\mathfrak{p} \in H^{(\sigma)}(E)$ אם ורק אם $\mathfrak{P} \in H^{(\tau\sigma)}(F)$ עבור איזה $\tau \in G$.

(ב) אם $\mathfrak{p} \in H^{(\sigma)}(E)$ אז $|\{\tau \in G | \ \mathfrak{P} \in H^{(\tau\sigma)}(F)\}| = e(\mathfrak{P}/\mathfrak{p})$.

נקבע $\mathfrak{P}/\mathfrak{p}$. נבחר אתר מייצג $\varphi_{\mathfrak{p}}$ של $\mathfrak{p}$ שהינו זהות על K ונרחיב אותו לאתר מייצג $\varphi_{\mathfrak{P}}$ של $\mathfrak{P}$. אז

$$\mathfrak{p} \in H^{(\sigma)}(E) \Leftrightarrow \varphi_{\mathfrak{p}} = \mathrm{Frob} \circ \varphi_{\mathfrak{p}} \circ \sigma, \qquad \mathfrak{P} \in H^{(\tau\sigma)}(F) \Leftrightarrow \varphi_{\mathfrak{P}} = \mathrm{Frob} \circ \varphi_{\mathfrak{P}} \circ \tau\sigma.$$

נניח $\varphi_{\mathfrak{P}} = \mathrm{Frob} \circ \varphi_{\mathfrak{P}} \circ \tau\sigma$. אז הצמצום ל־$E$ נותן $\varphi_{\mathfrak{p}} = \mathrm{Frob} \circ \varphi_{\mathfrak{p}} \circ \sigma$. להיפך, נניח $\varphi_{\mathfrak{p}} = \mathrm{Frob} \circ \varphi_{\mathfrak{p}} \circ \sigma$. אז $\mathrm{Frob} \circ \varphi_{\mathfrak{P}} \circ \sigma, \varphi_{\mathfrak{P}}$ שני אתרים של F/K שצמצומיהם ל־E שווים. לפי תרגיל 30.1, יש $\tau_0 \in G$ כך ש־$\varphi_{\mathfrak{P}} = \mathrm{Frob} \circ \varphi_{\mathfrak{P}} \circ \sigma\tau_0$. נגדיר $\tau = \sigma\tau_0\sigma^{-1}$. אז $\tau \in G$ ומתקיים $\varphi_{\mathfrak{P}} = \mathrm{Frob} \circ \varphi_{\mathfrak{P}} \circ \tau\sigma$. בכך הוכח (א).

אם גם $\tau' \in G$ מקיים זאת, אז $\varphi_{\mathfrak{P}} = \varphi_{\mathfrak{P}} \circ \tau'\tau^{-1}$. זה אומר, בסימונים של פרק 20, כי $\overline{\tau'\tau^{-1}} = 1$, כלומר, $\tau'\tau^{-1} \in I(\mathfrak{P}/\mathfrak{p})$. לפי מסקנה 20.11(ג), $|I(\mathfrak{P}/\mathfrak{p})| = e(\mathfrak{P}/\mathfrak{p})$. בכך הוכח (ב). ∎

משפט 31.2: *יהי* $\sigma \in \mathrm{Aut}(F/K)$*. נניח שיש הרחבה* $\hat{F}/K$ *של* F/K *ו־* $x \in F \smallsetminus K$ *כך ש־*

(א) $\sqrt{q} \in \mathbb{N}$.

(ב) $q > (\hat{g}+1)^4$*, באשר* $\hat{g}$ *הגזע של* $\hat{F}/K$.

(ג) *ל־* $\hat{F}/K$ *יש מחלק ראשוני ממעלה* 1.

(ד) $\sigma(x) = x$ *ו־* $\hat{F}/K(x)$ *הרחבת גלואה סופית.*

אז

$$.N^{(\sigma)}(F) - (q+1) > -[\hat{F} : K(x)](2\hat{g}+1)\sqrt{q}$$

הוכחה: נסמן $E = K(x)$, $n = [\hat{F} : E]$, ו־$G = \mathrm{Gal}(\hat{F}/E), H = \mathrm{Gal}(\hat{F}/F)$. נשים לב ש־$\sigma \in G$.

נניח תחילה כי $F = \hat{F}$ (ואז $H = 1$). לפי למה 31.1, עבור $\hat{F}/E$ ואוטומורפיזם הזהות,

$$.n(q+1) = nN(E) = nN^{(1)}(E) = \sum_{\tau \in G} N^{(\tau)}(\hat{F}) \tag{2}$$

במשפט 29.1 הוכחנו, לכל $\tau \in G$, $N^{(\tau)}(\hat{F}) - (q+1) < (2\hat{g}+1)\sqrt{q}$. לכן (לכל $\sigma \in G$)

$$\begin{aligned} N^{(\sigma)}(\hat{F}) &= \sum_{\tau \in G} N^{(\tau)}(\hat{F}) - \sum_{\sigma \neq \tau \in G} N^{(\tau)}(\hat{F}) \geq \\ &\geq n(q+1) - (n-1)\big((q+1) + (2\hat{g}+1)\sqrt{q}\big) \\ &= (q+1) - (n-1)(2\hat{g}+1)\sqrt{q} > (q+1) - n(2\hat{g}+1)\sqrt{q} \end{aligned} \tag{3}$$

כנדרש. במקרה הכללי, לפי למה 31.1 (עבור $\hat{F}/F$)

$$.N^{(\sigma)}(F) = \frac{1}{|H|} \sum_{\tau \in H} N^{(\tau\sigma)}(\hat{F})$$

בַּסְכום יש $|H|$ מחוברים, ולפי (3) כל אחד מהם גדול מאגף ימין של (3). לכן גם $N^{(\sigma)}(F)$ גדול ממנו. ∎

הוכחה של השערת רימן לשדות פונקציות (משפט 27.3): לפי משפט 28.1 די להוכיח את ההשערה עבור הרחבת שדות המקדמים F'/K' של F/K, באשר K'/K הרחבה סופית.

לפי תרגיל 30.3 יש $x \in F$ כך ש־F הרחבה פרידה סופית של $E = K(x)$. תהי $\hat{F}$ הרחבת גלואה סופית של E שמכילה את F (למשל, סגור גלואה של F/E) ויהי $\hat{K}$ הסגור האלגברי של K בתוך $\hat{F}$. אז $\hat{F}/\hat{K}$ הרחבה סופית של שדות פונקציות של F/K (לא הרחבת שדות המקדמים, אולי). לפי למה 19.3, $\hat{K}/K$ הרחבה סופית. לפי הפסקה הקודמת נוכל להחליף את K ב־$\hat{K}$ ואת F ב־$F\hat{K}$, ועל ידי כך להניח כי $\hat{K} = K$.

כזכור, g הוא הגזע של F/K. יהי $\hat{g}$ הגזע של $\hat{F}/K$.

יהי $K' = K_\ell$ באשר ℓ זוגי גדול מספיק. אז $|K'| = q^\ell$. הגזע אינו משתנה בהרחבות שדות המקדמים. לכן אם נחליף את F/K ואת $\hat{F}/K$ ב־FK'/K' ו־$\hat{F}K'/K'$, נוכל להניח

$$\begin{tikzcd}[arrows=-]
 & \hat{F} \\
F \arrow[r] \arrow[d] & F\hat{K} \arrow[u] \arrow[d] \\
E \arrow[r] \arrow[d] & E\hat{K} \arrow[d] \\
K \arrow[r] & \hat{K}
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=-]
\hat{F} \arrow[r] \arrow[d] & \hat{F}K' \arrow[d] \\
F \arrow[r] \arrow[d] & FK' \arrow[d] \\
E \arrow[r] \arrow[d] & EK' \arrow[d] \\
K \arrow[r] & K'
\end{tikzcd}$$

(א) $\sqrt{q} \in \mathbb{N}$.

(ב) $q > (\hat{g}+1)^4$, $q > (g+1)^4$.

(ג) ל־$\hat{F}/K$, ולכן גם ל־F/K, יש מחלק ראשוני ממעלה 1.

יתר על כן, יהי $r \in \mathbb{N}$. תנאים (א)־(ג) נכונים גם אם נחליף את K ב־K_r ואת $F, \hat{F}$ בהרחבות שדות המקדמים $FK_r, \hat{F}K_r$.

יהי $c = \max\big((2g+1), [\hat{F} : K(x)](2\hat{g}+1)\big)$. במשפט 29.1 הוכחנו

$$N(F_r) - (q^r+1) < cq^{\frac{r}{2}}. \tag{4}$$

במשפט 31.2 הוכחנו

$$N(F_r) - (q^r+1) > -cq^{\frac{r}{2}}. \tag{5}$$

מתוך (4) ו־(5) נקבל

$$|N(F_r) - (q^r+1)| < cq^{\frac{r}{2}}.$$

לפי משפט 28.2 זה מוכיח את ההשערה עבור F/K. ∎

32. הדיפרנט

תהי F/L הרחבת שדות פונקציות סופית של E/K. (כלומר, F/E הרחבה סופית, ולכן L/K הרחבה סופית, לפי למה 19.3.) נניח ש־F/E הרחבה פרידה. אז גם L/K פרידה:

תרגיל 32.1: *תהי F/L הרחבת שדות פונקציות סופית של E/K. אם F/E פרידה, אז L/K פרידה.*

הוכחה: יהי $\alpha \in L$ ויהי $f \in K[X]$ הפולינום האי פריק של α מעל K. לפי תרגיל 6.7, f אי פריק גם מעל E. כיוון ש־$\alpha \in F$ פריד מעל E, אין ל־f שורשים כפולים מעל E, ולכן גם לא מעל K. לכן α פריד מעל K. ∎

תזכורת 32.2: יהי R תחום שלמות ויהי K שדה המנות שלו. תהי L/K הרחבת שדות. איבר $x \in L$ הוא **שלם מעל** R אם x שורש של פולינום מתוקן עם מקדמים ב־R. זה שקול לכך ש־$R[x]$ הינו מודול־R נוצר סופית, וגם לכך ש־$R[x]$ מוכל בתת חוג C של L שהינו מודול־R נוצר סופית.

קבוצת כל האיברים של L השלמים מעל R נקראת **הסגור השלם של** R **ב־**L. מהאפיון השקול של השלמות מהפסקה הקודמת יוצא שהסגור השלם הוא חוג אשר מכיל את R.

החוג R נקרא **סגור בשלמות** אם הסגור השלם של R בשדה המנות שלו K הוא R.

אם R סגור בשלמות ו־$x \in L$ שלם מעליו, אז $\mathrm{irr}(x, K)$, הפולינום האי פריק של x מעל K, הוא פולינום מעל R. (אכן, הצמודים של x מעל K הם גם שלמים מעל R, והמקדמים של $\mathrm{irr}(x, K)$ הם סכומים של מכפלות של הצמודים האלה, לכן גם הם שלמים מעל R, כלומר, הם בסגור השלם R' של R ב־K; אבל $R' \cap K = R$, לכן המקדמים של $\mathrm{irr}(x, K)$ הם ב־R.)

תרגיל 32.3: *אם K שדה מנות של חוג R ו־x אלגברי מעל K, אז יש $0 \neq a \in R$ כך ש־ax שלם מעל R.*

דוגמה 32.4: חוג הערכה הינו סגור בשלמות. אכן, יהי R חוג הערכה ויהי K שדה המנות שלו. יהי $x \in K$ שלם מעל R. אז יש $a_0, \dots, a_{n-1} \in R$ כך ש־$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. מכאן $x = -a_{n-1} - \cdots - a_1(x^{-1})^{n-2} - a_0(x^{-1})^{n-1}$. לכן, אם $x^{-1} \in R$, אז $x \in R$. אם $x^{-1} \notin R$, אז $x \in R$, בגלל ש־R חוג הערכה. ∎

למה 32.5: *יהי R תת חוג של שדה L. אז הסגור השלם של R ב־L הוא החיתוך של כל חוגי ההערכה של L שמכילים את R.*

הוכחה: יהי $\mathcal{O}$ חוג הערכה של L שמכיל את R. אם $x \in L$ שלם מעל R, אז הוא גם שלם מעל $\mathcal{O}$, וכיוון ש־$\mathcal{O}$ סגור בשלמות, $x \in \mathcal{O}$.

להיפך, יהי $x \in L$ שאינו שלם מעל R. אז $x \notin \hat{R} := R[x^{-1}]$ (מנימוק דומה לנימוק בדוגמה 32.4 – אם $x = -a_{n-1} - \cdots - a_1(x^{-1})^{n-2} - a_0(x^{-1})^{n-1} \in \hat{R}$, אז $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$). בפרט x^{-1} אינו הפיך ב־$\hat{R}$. לכן הוא מוכל באידאל מקסימלי m של $\hat{R}$. אז $k = \hat{R}/m$ הוא שדה. את העתקת המנה $\hat{R} \to k$ ניתן להרחיב לאתר φ של L (לתוך הסגור האלגברי של k), לפי משפט 3.2(א). מתקיים $\varphi(x^{-1}) = 0$, לכן $\varphi(x) = \infty$. לכן חוג ההערכה של L המתאים ל־φ (אשר מכיל את $\hat{R}$) אינו מכיל את x. ∎

תזכורת 32.6: תהי L/K הרחבה סופית פרידה. העתקת **העקבה** $\mathrm{tr}_{L/K} : L \to K$ מוגדרת על ידי

$$\mathrm{tr}_{L/K}(x) = \sum_\sigma \sigma(x),$$

באשר σ עובר על כל השיכוני־K של L לתוך סגור אלגברי של K. (יש $[L:K]_s = [L:K]$ שיכונים כאלה. נשים לב ש־$\mathrm{tr}_{L/K}$ היא אכן לתוך K.) זוהי העתקה לינארית־K, כי כל σ הוא העתקה לינארית־K. העקבה איננה העתקת האפס (כי היא סכום של קרקטרים שונים של החבורה $L^\times$, ואלה בלתי תלויים לינארית מעל L), לכן היא על.

אם L'/L הרחבה סופית פרידה נוספת, אז $\mathrm{tr}_{L'/K} = \mathrm{tr}_{L/K} \circ \mathrm{tr}_{L'/L}$.

נתבונן ב־L כמרחב וקטורי מעל K. יהי $L^* = \mathrm{Hom}_K(L,K)$ המרחב הדואלי של L. כל $x \in L$ מגדיר $\varphi_x \in L^*$ על ידי $\varphi_x(y) = \mathrm{tr}_{L/K}(xy)$. (זוהי הרכבה של שתי העתקות לינאריות K: ההכפלה ב־x ו־$\mathrm{tr}_{L/K}$). יתר על כן, ההעתקה $x \mapsto \varphi_x$ היא העתקה לינארית חד חד ערכית; כיוון ש־$\dim_K L = \dim_K L^* < \infty$, העתקה זו היא איזומורפיזם $L \to L^*$.

בפרט, לכל בסיס $z_1, \dots, z_n$ של L מעל K יש **בסיס דואלי** $z_1^*, \dots, z_n^*$ של L^* מעל K, שמאופיין על ידי $\mathrm{tr}_{L/K}(z_i^* z_j) = \delta_{ij}$.

אם R תת חוג של K ו־$x \in L$ שלם מעליו, אז גם $\mathrm{tr}_{K/L}(x) \in K$ שלם מעל R. בפרט,

(א) אם R סגור בשלמות, ו־$x \in L$ שלם מעל R, אז $\mathrm{tr}_{L/K}(x) \in R$. ∎

משפט 32.7: *יהי $t \in \mathcal{O}_\mathfrak{p}$ כך ש־$v_\mathfrak{p}(t) = 1$. בתנאים לעיל, עבור כל $\mathfrak{p}$*

(א) $\mathcal{O}'_\mathfrak{p} = \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_\mathfrak{P}$.

(ב) *$\mathcal{O}_\mathfrak{p}$ ו־$\mathcal{O}'_\mathfrak{p}$ הם חוגים ראשיים. אם $0 \neq I \subseteq \mathcal{O}_\mathfrak{p}$ אידאל, אז $I = t^k \mathcal{O}_\mathfrak{p}$, באשר $k \geq 0$.*

(ג) *אם $0 \neq I \subseteq E$ מודול־$\mathcal{O}_\mathfrak{p}$ כך של־$v_\mathfrak{p}(I)$ יש חסם מלרע, אז $I = t^k \mathcal{O}_\mathfrak{p}$, באשר $k \in \mathbb{Z}$.*

(ד) *יהי $z_1, \dots, z_n$ בסיס של F/E כך ש־$\sum_{j=1}^n \mathcal{O}_\mathfrak{p} z_j \subseteq \mathcal{O}'_\mathfrak{p}$. אז $\mathcal{O}'_\mathfrak{p} \subseteq \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i^*$.*

(ה) *יש בסיס $z_1, \dots, z_n$ של F/E כך ש־$\mathcal{O}'_\mathfrak{p} = \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i$.*

הוכחה: (א) למה 32.5.

(ב) לפי (א), $\mathcal{O}'_\mathfrak{p} = \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_\mathfrak{P}$. נוכיח שאגף ימין הוא חוג ראשי.

יהי $0 \neq I$ אידאל של $\mathcal{O}'_\mathfrak{p}$. לכל $\mathfrak{P}/\mathfrak{p}$ נבחר $x_\mathfrak{P} \in I$ כך ש־$v_\mathfrak{P}(x_\mathfrak{P}) = k_\mathfrak{P} := \min\{v_\mathfrak{P}(I)\}$. בפרט $x_\mathfrak{P} \in I \subseteq \mathcal{O}'_\mathfrak{P}$, ולכן $v_{\mathfrak{P}'}(x_\mathfrak{P}) \geq 0$, לכל $\mathfrak{P}'/\mathfrak{p}$. לפי משפט הקירוב החלש לכל $\mathfrak{P}/\mathfrak{p}$ יש $z_\mathfrak{P} \in F$ כך ש־

$$v_\mathfrak{P}(z_\mathfrak{P}) = 0, \qquad v_{\mathfrak{P}'}(z_\mathfrak{P}) > k_{\mathfrak{P}'} \geq 0 \text{ לכל } \mathfrak{P}' \neq \mathfrak{P}$$

אז $z_\mathfrak{P} \in \mathcal{O}'_\mathfrak{p}$, ולכן $x := \sum_\mathfrak{P} x_\mathfrak{P} z_\mathfrak{P} \in I$. מכאן $x\mathcal{O}'_\mathfrak{p} \subseteq I$. נראה את ההכלה ההפוכה. יהי $z \in I$. אז כיוון ש־$v_\mathfrak{P}(x_\mathfrak{P} z_\mathfrak{P}) = k_\mathfrak{P} + 0 = k_\mathfrak{P}$ ו־$v_\mathfrak{P}(x_{\mathfrak{P}'} z_{\mathfrak{P}'}) > 0 + k_\mathfrak{P} = k_\mathfrak{P}$ לכל $\mathfrak{P}' \neq \mathfrak{P}$, מתקיים $v_\mathfrak{P}(x) = k_\mathfrak{P}$ לכל $\mathfrak{P}/\mathfrak{p}$. אז $v_\mathfrak{P}(\frac{z}{x}) = v_\mathfrak{P}(z) - k_\mathfrak{P} \geq 0$ לכל $\mathfrak{P}$. לכן $\frac{z}{x} \in \mathcal{O}'_\mathfrak{p}$ ולכן $z = x\frac{y}{x} \in x\mathcal{O}'_\mathfrak{p}$.

לכן $\mathcal{O}'_\mathfrak{p}$ ראשי. אם $F = E$, אז $\mathcal{O}'_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$, לכן גם $\mathcal{O}_\mathfrak{p}$ ראשי. אם נחזור על ההוכחה במקרה זה (בו $\mathfrak{p} =: \mathfrak{P}$ הוא המחלק היחיד מעל $\mathfrak{p}$) עם $k = k_\mathfrak{P}$, $x_\mathfrak{P} = t^k$, ו־$z_\mathfrak{P} = 1$, אז $x = x_\mathfrak{P} z_\mathfrak{p} = t^k$.

(ג) לפי ההנחה יש $r \in \mathbb{Z}$ כך ש־$v_\mathfrak{p}(I) \geq r = v_\mathfrak{p}(t^r)$. אז $v_\mathfrak{p}(t^{-r}I) \geq 0$, לכן $t^{-r}I \subseteq \mathcal{O}_\mathfrak{p}$. לכן $t^{-r}I$ הוא מודול־$\mathcal{O}_\mathfrak{p}$ מוכל ב־$\mathcal{O}_\mathfrak{p}$, כלומר, אידאל של $\mathcal{O}_\mathfrak{p}$. לפי (ב) יש $k \geq 0$ כך ש־$t^{-r}I = t^k\mathcal{O}_\mathfrak{p}$. לכן $I = t^{k+r}\mathcal{O}_\mathfrak{p}$.

(ד) לכל $z \in F$ יש $a_1, \ldots, a_n \in E$ כך ש־$z = \sum_{i=1}^n a_i z_i^*$.

אם $z \in \mathcal{O}'_\mathfrak{p}$, אז, לכל j, $zz_j \in \mathcal{O}'_\mathfrak{p}$, לכן $\mathrm{tr}_{F/E}(zz_j) \in \mathcal{O}_\mathfrak{p}$, לפי תזכורת 32.6(א). אבל

$$\mathcal{O}_\mathfrak{p} \ni \mathrm{tr}_{F/E}(zz_j) = \mathrm{tr}_{F/E}\Big(\sum_{i=1}^n a_i z_i^* z_j\Big) = \sum_{i=1}^n a_i \,\mathrm{tr}_{F/E}(z_i^* z_j) = \sum_{i=1}^n a_i\delta_{ij} = a_j.$$

לכן $z = \sum_{i=1}^n a_i z_i^* \in \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i^*$.

(ה) נבחר בסיס $z_1, \ldots, z_n$ של F/E. לפי תרגיל 32.3, בלי הגבלת הכלליות $z_1, \ldots, z_n \in \mathcal{O}'_\mathfrak{p}$. כלומר, $\sum_{j=1}^n \mathcal{O}_\mathfrak{p} z_j \subseteq \mathcal{O}'_\mathfrak{p}$. נוכיח באינדוקציה על k את הטענה הבאה:

טענה 1: יש $u_1, \ldots, u_n \in \mathcal{O}'_\mathfrak{p}$, כך ש־$\sum_{i=1}^k \mathcal{O}_\mathfrak{p} u_i = \mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^k \mathcal{O}_\mathfrak{p} z_i^*$ לכל $0 \leq k \leq n$.

עבור $k = 0$ זה ברור ($0 = 0$).

נניח שכבר מצאנו $u_1, \ldots, u_{k-1} \in \mathcal{O}'_\mathfrak{p}$ כך ש־ $\sum_{i=1}^{k-1} \mathcal{O}_\mathfrak{p} u_i = \mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^{k-1} \mathcal{O}_\mathfrak{p} z_i^*$. הקבוצה

$$I = \{a_k \in \mathcal{O}_\mathfrak{p} |\ \text{קיימים } a_1, \ldots, a_{k-1} \in \mathcal{O}_\mathfrak{p} \text{ כך ש־} a_1 z_1^* + \cdots + a_{k-1} z_{k-1}^* + a_k z_k^* \in \mathcal{O}'_\mathfrak{p}\}$$

היא אידאל של $\mathcal{O}_\mathfrak{p}$. לפי (ב), $\mathcal{O}_\mathfrak{p}$ הוא חוג ראשי, לכן יש $a_k \in \mathcal{O}_\mathfrak{p}$ כך ש־ $I = a_k\mathcal{O}_\mathfrak{p}$. כיוון ש־$a_k \in I$, יש $a_1, \ldots, a_{k-1} \in \mathcal{O}_\mathfrak{p}$ כך ש־ $u_k := a_1 z_1^* + \cdots + a_{k-1} z_{k-1}^* + a_k z_k^* \in \mathcal{O}'_\mathfrak{p}$. לפי משוואה זו ולפי הנחת האינדוקציה $\sum_{i=1}^k \mathcal{O}_\mathfrak{p} u_i \supseteq \mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^k \mathcal{O}_\mathfrak{p} z_i^*$. להיפך, יהי $z \in \mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^k \mathcal{O}_\mathfrak{p} z_i^*$. אז $z = b_1 z_1^* + \cdots + b_k z_k^*$, באשר $b_1, \ldots, b_k \in \mathcal{O}_\mathfrak{p}$. לכן $b_k \in I$, לכן יש $c \in \mathcal{O}_\mathfrak{p}$ כך ש־$b_k = ca_k$ ואז

$$z - cu_k = (b_1 - ca_1)z_1^* + \cdots + (b_{k-1} - ca_{k-1})z_{k-1}^* + (b_k - ca_k)z_k^* \in \mathcal{O}'_\mathfrak{p} \cap \sum_{i=1}^{k-1} \mathcal{O}_\mathfrak{p} z_i^* = \sum_{i=1}^{k-1} \mathcal{O}_\mathfrak{p} u_i,$$

לכן $z \in \sum_{i=1}^k \mathcal{O}_\mathfrak{p} u_i$.

לפי (ד), $\mathcal{O}'_\mathfrak{p} \subseteq \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i^*$. לכן עבור $k = n$ טענה 1 נותנת $\mathcal{O}'_\mathfrak{p} = \sum_{i=1}^n \mathcal{O}_\mathfrak{p} u_i$. לפי תרגיל 32.3, כל איבר של F הוא מהצורה $\frac{z}{a}$, באשר $z \in \mathcal{O}'_\mathfrak{p}$ ו־$a \in \mathcal{O}_\mathfrak{p}$. לכן $F = \sum_{i=1}^n E u_i$, ולכן $u_1, \ldots, u_n$ בסיס של F/E. ∎

הגדרה 32.8: יהי $\mathfrak{p}$ מחלק ראשוני של E/K. יהי $\mathcal{O}_\mathfrak{p}$ חוג ההערכה שלו ויהי $\mathcal{O}'_\mathfrak{p}$ הסגור השלם של $\mathcal{O}_\mathfrak{p}$ ב־F. אז

$$\mathcal{C}_\mathfrak{p} := \{z \in F |\ \mathrm{tr}_{F/E}(z\mathcal{O}'_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}\}$$

נקרא **המודול המשלים מעל** $\mathcal{O}_\mathfrak{p}$. זהו מודול־$\mathcal{O}'_\mathfrak{p}$ ולכן גם מודול־$\mathcal{O}_\mathfrak{p}$.

משפט 32.9: *בתנאים לעיל, עבור כל* $\mathfrak{p} \in \mathbb{P}(E)$,

(א) $\mathcal{O}'_\mathfrak{p} \subseteq \mathcal{C}_\mathfrak{p}$.

(ב) *יהי* $z_1, \ldots, z_n$ *בסיס של* F/E *כך ש־* $\mathcal{O}'_\mathfrak{p} = \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i$. *אז* $\mathcal{C}_\mathfrak{p} = \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i^*$.

(ג) *יש* $t_\mathfrak{p} \in F$ *כך ש־* $\mathcal{C}_\mathfrak{p} = t_\mathfrak{p} \mathcal{O}'_\mathfrak{p}$.

(ד) *אם* $\mathcal{C}_\mathfrak{p} = t\mathcal{O}'_\mathfrak{p}$*, אז* $v_\mathfrak{P}(t) \le 0$ *לכל* $\mathfrak{P}$ *של* F/L *שמונח מעל* $\mathfrak{p}$.

(ה) *אם* $\mathcal{C}_\mathfrak{p} = t\mathcal{O}'_\mathfrak{p}$*, ו־* $t' \in F$ *כלשהו, אז* $\mathcal{C}_\mathfrak{p} = t'\mathcal{O}'_\mathfrak{p} \quad \Leftrightarrow \quad v_\mathfrak{P}(t') = v_\mathfrak{P}(t)$ *לכל* $\mathfrak{P}/\mathfrak{p}$.

בנוסף לכך

(ו) $\mathcal{C}_\mathfrak{p} = \mathcal{O}'_\mathfrak{p}$ *עבור כמעט כל* $\mathfrak{p}$.

הוכחה: (א) יהי $z \in \mathcal{O}'_\mathfrak{p}$. אז $z\mathcal{O}'_\mathfrak{p} \subseteq \mathcal{O}'_\mathfrak{p}$, לכן $\mathrm{tr}_{F/E}(z\mathcal{O}'_\mathfrak{p}) \subseteq \mathrm{tr}_{F/E}(\mathcal{O}'_\mathfrak{p}) \subseteq \mathcal{O}_\mathfrak{p}$, לפי תזכורת 32.6(א). לכן $z \in \mathcal{C}_\mathfrak{p}$.

(ב) יהי $z \in \mathcal{C}_\mathfrak{p}$. אז יש $x_1, \ldots, x_n \in E$ כך ש־ $z = \sum_{i=1}^n x_i z_i^*$. לפי הגדרת $\mathcal{C}_\mathfrak{p}$ מתקיים $\mathrm{tr}_{F/E}(zz_j) \in \mathcal{O}_\mathfrak{p}$ לכל j. אבל

$$\mathcal{O}_\mathfrak{p} \ni \mathrm{tr}_{F/E}(zz_j) = \mathrm{tr}_{F/E}\big(\sum_{i=1}^n x_i z_i^* z_j\big) = \sum_{i=1}^n x_i \,\mathrm{tr}_{F/E}(z_i^* z_j) = \sum_{i=1}^n x_i \delta_{ij} = x_j$$

לכן $z \in \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i^*$.

להיפך, אם $z \in \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i^*$ ו־ $z' \in \mathcal{O}'_\mathfrak{p}$, נאמר, $z = \sum_{i=1}^n x_i z_i^*$ ו־ $z' = \sum_{j=1}^n y_j z_j$, באשר $x_i, y_j \in \mathcal{O}_\mathfrak{p}$, אז

$$\mathrm{tr}_{F/E}(zz') = \mathrm{tr}_{F/E}\big(\sum_{i,j=1}^n x_i y_j z_i^* z_j\big) = \sum_{i,j=1}^n x_i y_j \,\mathrm{tr}_{F/E}(z_i^* z_j) =$$
$$= \sum_{i,j=1}^n x_i y_j \delta_{ij} = \sum_{i=1}^n x_i y_i \in \mathcal{O}_\mathfrak{p}$$

לכן $z \in \mathcal{C}_\mathfrak{p}$.

(ג) לפי (ב) יש בסיס $z_1^*, \ldots, z_n^*$ של F/E כך ש־ $\mathcal{C}_\mathfrak{p} = \sum_{i=1}^n \mathcal{O}_\mathfrak{p} z_i^*$. נבחר $x \in E$ כך ש־ $v_\mathfrak{p}(x) \ge -v_\mathfrak{P}(z_i^*)$ לכל $\mathfrak{P}/\mathfrak{p}$ ולכל i. אז

$$v_\mathfrak{P}(xz_i^*) = e(\mathfrak{P}/\mathfrak{p}) v_\mathfrak{p}(x) + v_\mathfrak{P}(z_i^*) \ge v_\mathfrak{p}(x) + v_\mathfrak{P}(z_i^*) \ge 0$$

לכל $\mathfrak{P}/\mathfrak{p}$ ולכל i. לכן $x\mathcal{C}_\mathfrak{p} \subseteq \mathcal{O}'_\mathfrak{p}$. ברור ש־ $x\mathcal{C}_\mathfrak{p}$ הוא אידאל של $\mathcal{O}'_\mathfrak{p}$. לפי משפט 32.7(ב), $\mathcal{O}'_\mathfrak{p}$ הוא חוג ראשי. לכן יש $y \in \mathcal{O}'_\mathfrak{p}$ כך ש־ $x\mathcal{C}_\mathfrak{p} = y\mathcal{O}'_\mathfrak{p}$. מכאן $\mathcal{C}_\mathfrak{p} = \frac{y}{x}\mathcal{O}'_\mathfrak{p}$.

(ד) נניח $\mathcal{C}_\mathfrak{p} = t\mathcal{O}'_\mathfrak{p}$. לפי (א), $\mathcal{O}'_\mathfrak{p} \subseteq t\mathcal{O}'_\mathfrak{p}$. מכאן $\frac{1}{t} \in \frac{1}{t}\mathcal{O}'_\mathfrak{p} \subseteq \mathcal{O}'_\mathfrak{p} = \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_\mathfrak{P}$ לכן $v_\mathfrak{P}(\frac{1}{t}) \ge 0$ לכל $\mathfrak{P}$ של F/L שמונח מעל $\mathfrak{p}$.

(ה) $v_{\mathfrak{P}}(\frac{t}{t'}) \geq 0$ לכל $\mathfrak{P}/\mathfrak{p} \Leftrightarrow \frac{t}{t'} \in \mathcal{O}'_\mathfrak{p} = \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_\mathfrak{P} \Leftrightarrow \frac{t}{t'}\mathcal{O}'_\mathfrak{p} \subseteq \mathcal{O}'_\mathfrak{p} \Leftrightarrow t\mathcal{O}'_\mathfrak{p} \subseteq t'\mathcal{O}'_\mathfrak{p}$. לכן $v_{\mathfrak{P}}(t) = v_{\mathfrak{P}}(t')$ לכל $\mathfrak{P}/\mathfrak{p} \Leftrightarrow v_{\mathfrak{P}}(\frac{t}{t'}) = 0$ לכל $\mathfrak{P}/\mathfrak{p} \Leftrightarrow t\mathcal{O}'_\mathfrak{p} = t'\mathcal{O}'_\mathfrak{p}$.

(ו) יהי $z_1, \ldots, z_n$ בסיס של F/E ויהי $z_1^*, \ldots, z_n^*$ הבסיס הדואלי שלו. תהי S קבוצת כל הקטבים $\mathfrak{p} \in \mathbb{P}(E)$ של המקדמים של הפולינומים האי פריקים של $z_1, \ldots, z_n, z_1^*, \ldots, z_n^*$ מעל E. אז S קבוצה סופית. אם $\mathfrak{p} \in \mathbb{P}(E) \smallsetminus S$, אז המקדמים האלה נמצאים ב־$\mathcal{O}_\mathfrak{p}$ ולכן $z_1, \ldots, z_n, z_1^*, \ldots, z_n^* \in \mathcal{O}'_\mathfrak{p}$. מכאן הכלות (3) ו(1) ב־,

$$\sum_i \mathcal{O}_\mathfrak{p} z_i \subseteq^{(1)} \mathcal{O}'_\mathfrak{p} \subseteq^{(2)} \sum_i \mathcal{O}_\mathfrak{p} z_i^* \subseteq^{(3)} \mathcal{O}'_\mathfrak{p} \subseteq^{(4)} \sum_i \mathcal{O}_\mathfrak{p} z_i.$$

הכלה (2) נובעת ממשפט 32.7(ד). גם הכלה (4) נובעת מאותו הנימוק, כי $z_i = (z_i^*)^*$.

לכן כל ההכלות הן שוויונות. לפי (ב), $\mathcal{C}_\mathfrak{p} = \mathcal{O}'_\mathfrak{p}$. ∎

הגדרה 32.10: יהי $\mathfrak{p}$ מחלק ראשוני של E/K. יהי $\mathcal{O}_\mathfrak{p}$ חוג ההערכה שלו, $\mathcal{O}'_\mathfrak{p}$ הסגור השלם של $\mathcal{O}_\mathfrak{p}$ ב־F, ו־$\mathcal{C}_\mathfrak{p} = t_\mathfrak{p}\mathcal{O}'_\mathfrak{p}$ המודול המשלים מעל $\mathcal{O}_\mathfrak{p}$. אז נגדיר

(א) לכל מחלק $\mathfrak{P}$ מעל $\mathfrak{p}$ **מעריך הדיפרנט של $\mathfrak{P}$ מעל** $\mathfrak{p}$: $d(\mathfrak{P}/\mathfrak{p}) := -v_\mathfrak{P}(t_\mathfrak{p})$;

(ב) **הדיפרנט של** F/E: $\mathrm{Diff}(F/E) := \sum_{\mathfrak{p}\in\mathbb{P}(E)} \sum_{\mathfrak{P}/\mathfrak{p}} d(\mathfrak{P}/\mathfrak{p})\mathfrak{P}$. ∎

הערה 32.11: (א) לפי משפט 32.9(ה) $d(\mathfrak{P}/\mathfrak{p})$ מוגדר היטב (אינו תלוי בבחירת $t_\mathfrak{p}$). לפי משפט 32.9(ד), $d(\mathfrak{P}/\mathfrak{p}) \geq 0$.

(ב) לפי משפט 32.9(ו), $d(\mathfrak{P}/\mathfrak{p}) = 0$ עבור כמעט כל $\mathfrak{p}$ וכל $\mathfrak{P}/\mathfrak{p}$. לכן $\mathrm{Diff}(\mathfrak{P}/\mathfrak{p})$ הוא מחלק (אי שלילי) של F/L.

(ג) יהי $z \in F$. אז $v_\mathfrak{P}(z) \geq -d(\mathfrak{P}/\mathfrak{p})$ לכל $\mathfrak{P}/\mathfrak{p}$ $\quad\Leftrightarrow\quad z \in \mathcal{C}_\mathfrak{p}$.

אכן, יהי $t \in F$ כך ש־$\mathcal{C}_\mathfrak{p} = t\mathcal{O}'_\mathfrak{p}$. אז לפי משפט 32.7(א)

$$z \in \mathcal{C}_\mathfrak{p} \Leftrightarrow \frac{z}{t} \in \mathcal{O}'_\mathfrak{p} \Leftrightarrow \frac{z}{t} \in \bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_\mathfrak{P} \Leftrightarrow v_\mathfrak{P}(\frac{z}{t}) \geq 0 \text{ לכל } \mathfrak{P}/\mathfrak{p} \Leftrightarrow$$

$$\Leftrightarrow v_\mathfrak{P}(z) \geq v_\mathfrak{P}(t) = -d(\mathfrak{P}/\mathfrak{p}) \text{ לכל } \mathfrak{P}/\mathfrak{p}$$

∎

למה 32.12: *יהי $\mathfrak{p} \in \mathbb{P}(E)$ ויהיו $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ כל המחלקים הראשוניים מעליו. נסמן $\mathfrak{P} = \mathfrak{P}_1$ ותהי $\pi\colon \mathcal{O}_\mathfrak{P} \to F_\mathfrak{P}$ העתקת המנה המתאימה ל־$\mathfrak{P}$, אשר מרחיבה את העתקת המנה $\pi\colon \mathcal{O}_\mathfrak{p} \to E_\mathfrak{p}$ שמתאימה ל־$\mathfrak{p}$. יהי $y \in \mathcal{O}'_\mathfrak{p}$ כך ש־$v_{\mathfrak{P}_j}(y) > 0$ לכל $2 \leq j \leq r$ ו־$\pi(y)$ נמצא ב־$F_{\mathfrak{P},s}$, הסגור הפריד של $E_\mathfrak{p}$ בתוך $F_\mathfrak{P}$. אז*

$$\pi\big(\mathrm{tr}_{F/E}(y)\big) = e(\mathfrak{P}/\mathfrak{p})\, \mathrm{tr}_{F_{\mathfrak{P},s}/E_\mathfrak{p}}\big(\pi(y)\big).$$

הוכחה: יהי $\hat{F}$ סגור גלואה של F/E ויהי $\hat{\mathfrak{P}}$ מחלק ראשוני של $\hat{F}$ מעל $\mathfrak{P}$. נרחיב את π להעתקת המנה $\pi\colon \mathcal{O}_{\hat{\mathfrak{P}}} \to \hat{F}_{\hat{\mathfrak{P}}}$.

לפי ההגדרה, $\mathrm{tr}_{F/E}(y) = \sum_{i=1}^n \sigma_i(y)$, באשר $\sigma_1, \dots, \sigma_n \colon F \to \hat{F}$ כל שיכוני־E השונים. נרחיב אותם לאוטומורפיזמים של $\hat{F}$ מעל E באופן הבא: אם יש הרחבה σ_i כך ש־$\sigma_i \in D(\hat{\mathfrak{P}}/\mathfrak{p})$, נבחר כזאת. בלי הגבלת הכלליות σ_1 היא הזהות של $\hat{F}$.

יהי $1 \le i \le n$. מהו $\pi(\sigma_i y)$? נבדיל בין שני מקרים:

(א) נניח ש־$\sigma_i \hat{\mathfrak{P}} = \hat{\mathfrak{P}}$, כלומר, $\sigma_i \in D(\hat{\mathfrak{P}}/\mathfrak{p})$. במקרה זה $\pi(\sigma_i y) = \overline{\sigma_i}(\pi(y))$, באשר $\overline{\sigma_i}$ התמונה של σ_i תחת האפימורפיזם $D(\hat{\mathfrak{P}}/\mathfrak{p}) \to \mathrm{Aut}(\hat{F}_{\hat{\mathfrak{P}}}/E_{\mathfrak{p}}) = \mathrm{Gal}(\hat{F}_{\hat{\mathfrak{P}},s}/E_{\mathfrak{p}})$. הצמצום של $\overline{\sigma_i}$ ל־$F_{\mathfrak{P},s}$ הוא שיכון־$E_{\mathfrak{p}}$ $\hat{F}_{\hat{\mathfrak{P}}} \to F_{\mathfrak{P},s}$. זה מוכיח את ההכלה "$\subseteq$" בטענה הבאה:

טענה: $\{\alpha\big(\pi(y)\big) |\ \alpha \colon F_{\mathfrak{P},s} \to \hat{F}_{\hat{\mathfrak{P}}} \text{ שיכון־} E_{\mathfrak{p}}\} = \{\overline{\sigma_i}(\pi(y)) = \pi(\sigma_i y) |\ \sigma_i \in D(\hat{\mathfrak{P}}/\mathfrak{p})\}$.

אכן, יהי $\alpha \colon F_{\mathfrak{P},s} \to \hat{F}_{\hat{\mathfrak{P}}}$ שיכון־$E_{\mathfrak{p}}$. נרחיב אותו ל־$\hat{\alpha} \in \mathrm{Aut}(\hat{F}_{\hat{\mathfrak{P}}}/E_{\mathfrak{p}})$. לפי משפט 20.7(ב) יש $\sigma \in D(\hat{\mathfrak{P}}/\mathfrak{p}) \le \mathrm{Aut}(\hat{F}/E)$ כך ש־$\bar{\sigma} = \hat{\alpha}$. בפרט $\pi(\sigma y) = \alpha\big(\pi(y)\big)$. יש $1 \le i \le n$ יחיד כך ש־$\sigma|_F = \sigma_i|_F$, ואז יש $\tau \in \mathrm{Aut}(\hat{F}/F)$ כך ש־$\sigma = \sigma_i \tau$. לפי הבחירה, $\sigma_i \in D(\hat{\mathfrak{P}}/\mathfrak{p})$. מתקיים $\pi(\sigma_i y) = \pi(\sigma_i \tau y) = \pi(\sigma y) = \bar{\sigma}\big(\pi(y)\big) = \alpha\big(\pi(y)\big)$.

(ב) נניח $\sigma_i \hat{\mathfrak{P}} \ne \hat{\mathfrak{P}}$, או, באופן שקול, $\hat{\mathfrak{P}} \ne \sigma_i^{-1}\hat{\mathfrak{P}}$. אז המחלק $\mathfrak{P}_j$ של F שמונח מתחת ל־$\sigma_i^{-1}\hat{\mathfrak{P}}$ הינו שונה מ־$\mathfrak{P}$ (שמונח מתחת ל־$\hat{\mathfrak{P}}$), אחרת $\hat{\mathfrak{P}}, \sigma_i^{-1}\hat{\mathfrak{P}}$ שניהם מונחים מעל אותו מחלק של F, ולכן יש $\tau \in \mathrm{Aut}(\hat{F}/F)$ כך ש־$\tau\hat{\mathfrak{P}} = \sigma_i^{-1}\hat{\mathfrak{P}}$, כלומר, $\sigma_i\tau \in D(\hat{\mathfrak{P}})$. כיוון ש־$\sigma_i\tau|_F = \sigma_i|_F$, לפי הבחירה, $\sigma_i \in D(\hat{\mathfrak{P}})$, בסתירה ל־$\sigma_i\hat{\mathfrak{P}} \ne \hat{\mathfrak{P}}$.

לכן, לפי הנתון, $v_{\mathfrak{P}_j}(y) > 0$, ולכן $v_{\sigma_i^{-1}\hat{\mathfrak{P}}}(y) > 0$. אבל $v_{\sigma_i^{-1}\hat{\mathfrak{P}}}(y) = v_{\hat{\mathfrak{P}}}(\sigma_i y)$. לכן $v_{\hat{\mathfrak{P}}}(\sigma_i y) > 0$. מכאן $\sigma_i y \in \mathcal{O}_{\hat{\mathfrak{P}}}$ ו־$\pi(\sigma_i y) = 0$, במקרה זה.

לכן לפי תרגיל 20.13 (נסמן $\hat{D} = D(\hat{\mathfrak{P}}/\mathfrak{p})$ ו־$A = \{\alpha \colon F_{\mathfrak{P},s} \to \hat{F}_{\hat{\mathfrak{P}}} |\ \alpha \text{ שיכון־} E_{\mathfrak{p}}\}$)

$$\pi\big(\mathrm{tr}_{F/E}(y)\big) = \sum_{i=1}^n \pi\big(\sigma_i(y)\big) = \sum_{\substack{i=1\\ \sigma_i \in \hat{D}}}^n \overline{\sigma_i}\big(\pi(y)\big) = \sum_{\alpha \in A} |\{i |\ \sigma_i \in \hat{D},\ \overline{\sigma_i} = \alpha\}| \cdot \alpha\big(\pi(y)\big) =$$
$$= \sum_{\alpha \in A} e(\mathfrak{P}/\mathfrak{p}) \alpha\big(\pi(y)\big) = e(\mathfrak{P}/\mathfrak{p})\, \mathrm{tr}_{F_{\mathfrak{P},s}/E_{\mathfrak{p}}}\big(\pi(y)\big)$$

∎

הלמה הקודמת היא מקרה פרטי של הלמה הבאה, אותה לא נוכיח (וגם לא נזדקק לה):

למה 32.13: *נניח ש־K הוא שדה משוכלל. יהי $\mathfrak{p} \in \mathbb{P}(E)$ ויהיו $\mathfrak{P}_1, \dots, \mathfrak{P}_r \in \mathbb{P}(F)$ כל המחלקים הראשוניים מעליו. לכל $1 \le j \le r$ תהי $\pi_j \colon \mathcal{O}_{\mathfrak{P}_j} \to F_{\mathfrak{P}_j}$ העתקת המנה המתאימה ל־$\mathfrak{P}_j$, אשר מרחיבה את העתקת המנה $\pi \colon \mathcal{O}_{\mathfrak{p}} \to E_{\mathfrak{p}}$ שמתאימה ל־$\mathfrak{p}$. אז לכל $y \in \mathcal{O}'_{\mathfrak{p}}$ מתקיים*

$$\pi\big(\mathrm{tr}_{F/E}(y)\big) = \sum_{j=1}^r e(\mathfrak{P}_j/\mathfrak{p})\, \mathrm{tr}_{F_{\mathfrak{P}_j}/E_{\mathfrak{p}}}\big(\pi_j(y)\big)$$

משפט 32.14 (משפט הדיפרנט של דדקינד): *תהי F/L הרחבה פרידה סופית של שדה פונקציות E/K. יהי $\mathfrak{p} \in \mathbb{P}(E)$ ויהי $\mathfrak{P} \in \mathbb{P}(F)$ מעליו. אז*

(א) $d(\mathfrak{P}/\mathfrak{p}) \geq e(\mathfrak{P}/\mathfrak{p}) - 1$. *בפרט* $e(\mathfrak{P}/\mathfrak{p}) = 1 \Rightarrow d(\mathfrak{P}/\mathfrak{p}) = 0$.

(ב) $d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1$ *אם ורק אם* $\operatorname{char} K \nmid e(\mathfrak{P}/\mathfrak{p})$. *בפרט* $e(\mathfrak{P}/\mathfrak{p}) = 1 \Leftarrow d(\mathfrak{P}/\mathfrak{p}) = 0$.

הוכחה: (א) לפי משפט הקירוב החלש יש $z \in F$ כך שמתקיים

$$v_{\mathfrak{P}_i}(z) = 1 - e(\mathfrak{P}_i/\mathfrak{p}) \text{ לכל } \mathfrak{P}_i/\mathfrak{p}.$$

אם נראה ש־$z \in \mathcal{C}_\mathfrak{p} = t_\mathfrak{p}\mathcal{O}'_\mathfrak{p}$, אז $v_\mathfrak{P}(z) \geq v_\mathfrak{P}(t_\mathfrak{p})$, כלומר, $1 - e(\mathfrak{P}/\mathfrak{p}) \geq -d(\mathfrak{P}/\mathfrak{p})$, כנדרש.

יהי $\hat{F}$ סגור גלואה של F/E ויהי $\hat{L}$ הסגור האלגברי של K (או של L, היינו הך) בתוך $\hat{F}$. אז $\hat{F}/\hat{L}$ הרחבה נורמלית של E/K, והיא גם הרחבה של F/L. יהי $n = [F:E]$. יש n שיכוני־E של F לתוך הסגור האלגברי של F, נאמר, $\sigma_1, \ldots, \sigma_n$. נרחיב אותם ל־$\hat{F}$. אז הם אוטומורפיזמים של $\hat{F}$ מעל E, כי $\hat{F}/E$ נורמלית. נבחר $\hat{\mathfrak{P}} \in \mathbb{P}(\hat{F})$ מעל $\mathfrak{P} \in \mathbb{P}(F)$. לכל $1 \leq i \leq n$ יהי $\mathfrak{P}_i = (\sigma_i^{-1}\hat{\mathfrak{P}}) \cap F \in \mathbb{P}(F)$. אז $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ מעל $\mathfrak{p}$, לא בהכרח שונים.

יהי $x \in \mathcal{O}'_\mathfrak{p}$. אז x שלם מעל $\mathcal{O}_\mathfrak{p}$, לכן, לכל i, גם $\sigma_i(x) \in \hat{F}$ שלם מעל $\mathcal{O}_\mathfrak{p}$, ולכן $v_{\hat{\mathfrak{P}}}(\sigma_i(x)) \geq 0$. לכן

$$\begin{aligned} v_{\hat{\mathfrak{P}}}\big(\sigma_i(zx)\big) &= v_{\hat{\mathfrak{P}}}\big(\sigma_i(z)\big) + v_{\hat{\mathfrak{P}}}\big(\sigma_i(x)\big) \geq v_{\hat{\mathfrak{P}}}\big(\sigma_i(z)\big) = v_{\sigma_i^{-1}\hat{\mathfrak{P}}}(z) = \\ &= e(\sigma_i^{-1}\hat{\mathfrak{P}}/\mathfrak{P}_i)v_{\mathfrak{P}_i}(z) = e(\sigma_i^{-1}\hat{\mathfrak{P}}/\mathfrak{P}_i)\big(1 - e(\mathfrak{P}_i/\mathfrak{p})\big) > \\ &> -e(\sigma_i^{-1}\hat{\mathfrak{P}}/\mathfrak{P}_i)e(\mathfrak{P}_i/\mathfrak{p}) = -e(\sigma_i^{-1}\hat{\mathfrak{P}}/\mathfrak{p}) = -e(\hat{\mathfrak{P}}/\mathfrak{p}) \end{aligned}$$

לכן

$$e(\hat{\mathfrak{P}}/\mathfrak{p})v_\mathfrak{p}\big(\operatorname{tr}_{F/E}(zx)\big) = v_{\hat{\mathfrak{P}}}\big(\operatorname{tr}_{F/E}(zx)\big) = v_{\hat{\mathfrak{P}}}\Big(\sum_{i=1}^n \sigma_i(zx)\Big) > -e(\hat{\mathfrak{P}}/\mathfrak{p}).$$

מכאן $v_\mathfrak{p}\big(\operatorname{tr}_{F/E}(zx)\big) > -1$, כלומר, $v_\mathfrak{p}\big(\operatorname{tr}_{F/E}(zx)\big) \geq 0$. לכן $z \in \mathcal{C}_\mathfrak{p}$.

(ב) יהיו $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_r$ כל המחלקים הראשונים מעל $\mathfrak{p}$. נסמן $e_i = e(\mathfrak{P}_i/\mathfrak{p})$, לכל i, ו־$e = e_1$.

תחילה נניח ש־$\operatorname{char} K \nmid e$. אז די להוכיח ש־$d(\mathfrak{P}/\mathfrak{p}) < e$.

יהי $t_\mathfrak{p} \in F$ כך ש־$\mathcal{C}_\mathfrak{p} = t_\mathfrak{p}\mathcal{O}'_\mathfrak{p}$, אז $v_{\mathfrak{P}_i}(t_\mathfrak{p}) = -d(\mathfrak{P}_i/\mathfrak{p})$ לכל i.

טענה 1: *יש* $y \in \mathcal{O}'_\mathfrak{p}$ *כך ש־*

$$v_\mathfrak{P}(y) = 0 \tag{1}$$

$$v_{\mathfrak{P}_i}(y) \geq \max\{1, e_i + v_{\mathfrak{P}_i}(t_\mathfrak{p})\} > 0, \quad 2 \leq i \leq r \tag{2}$$

$$v_\mathfrak{p}\big(\operatorname{tr}_{F/E}(y)\big) = 0 \tag{3}$$

אכן, $F_{\mathfrak{P},s}/E_{\mathfrak{p}}$ הרחבה פרידה. לכן יש $y_0 \in \mathcal{O}_{\mathfrak{P}} \subseteq F$ כך ש־ $\pi(y_0) \in F_{\mathfrak{P},s}$ ו־$\mathrm{tr}_{F_{\mathfrak{P},s}/E_{\mathfrak{p}}}\left(\pi(y_0)\right) \neq 0$. בפרט $\pi(y_0) \neq 0$, ולכן $v_{\mathfrak{P}}(y_0) = 0$. לפי משפט הקירוב החלש יש $y \in F$ כך ש־ $v_{\mathfrak{P}}(y - y_0) > 0$ וכן (2). אז מתקיים גם (1) ולכן $y \in \bigcap_{i=1}^{r} \mathcal{O}_{\mathfrak{P}_i} = \mathcal{O}'_{\mathfrak{p}}$. לפי למה 32.12

$$\pi\big(\mathrm{tr}_{F/E}(y)\big) = e \cdot \mathrm{tr}_{F_{\mathfrak{P},s}/E_{\mathfrak{p}}}\left(\pi(y)\right) = e \cdot \mathrm{tr}_{F_{\mathfrak{P},s}/E_{\mathfrak{p}}}\left(\pi(y_0)\right) \neq 0$$

כי $e \neq 0$ ב־$E_{\mathfrak{p}}$ (!). מכאן (3). בכך הוכחה טענה 1.

אם נכפיל את y באיבר $x \in E$ כך ש־$v_{\mathfrak{p}}(x) = -1$ (ולכן $v_{\mathfrak{P}_i}(x) = -e_i$ לכל i), נקבל

טענה 2: *יש $y' \in F$ כך ש־*

$$v_{\mathfrak{P}}(y') = -e \tag{1'}$$

$$v_{\mathfrak{P}_i}(y') \geq v_{\mathfrak{P}_i}(t_{\mathfrak{p}}) = -d(\mathfrak{P}_i/\mathfrak{p}), \quad 2 \leq i \leq r \tag{2'}$$

$$v_{\mathfrak{p}}\big(\mathrm{tr}_{F/E}(y')\big) = -1 \tag{3'}$$

כאשר המשוואה האחרונה נובעת מכך ש־$\mathrm{tr}_{F/E}$ היא לינארית־K ולכן $\mathrm{tr}_{F/E}(xy) = x\,\mathrm{tr}_{F/E}(y)$.

לפי $(3')$, $y' \notin \mathcal{C}_{\mathfrak{p}} = t_{\mathfrak{p}}\mathcal{O}'_{\mathfrak{p}}$. לכן לפי $(2')$ ולפי הערה 32.11 לא יתכן ש־ $v_{\mathfrak{P}}(y') \geq v_{\mathfrak{P}}(t_{\mathfrak{p}}) = -d(\mathfrak{P}/\mathfrak{p})$. לכן, לפי $(1')$, $-e < -d(\mathfrak{P}/\mathfrak{p})$, כלומר, $d(\mathfrak{P}/\mathfrak{p}) < e$.

להיפך, נניח ש־$e \mid \mathrm{char}\,K$. צריך להוכיח ש־$d(\mathfrak{P}/\mathfrak{p}) \geq e$.

טענה 3: *יש $y \in \mathcal{O}'_{\mathfrak{p}}$ כך שלכל $z \in \mathcal{O}'_{\mathfrak{p}}$*

$$v_{\mathfrak{P}}(y) = 0,\ v_{\mathfrak{P}}(yz) \geq 0 \tag{4}$$

$$v_{\mathfrak{P}_i}(yz) > 0, \quad 2 \leq i \leq r \tag{5}$$

$$v_{\mathfrak{p}}\big(\mathrm{tr}_{F/E}(yz)\big) > 0 \tag{6}$$

אכן, לפי משפט הקירוב החלש יש $y \in F$ כך ש־ $v_{\mathfrak{P}}(y) = 0, v_{\mathfrak{P}_i}(y) > 0,\ 2 \leq i \leq r$. אז $y \in \mathcal{O}'_{\mathfrak{p}}$. אם $z \in \mathcal{O}'_{\mathfrak{p}}$, אז $v_{\mathfrak{P}_i}(z) \geq 0$ לכל i, ומכאן $(4), (5)$. כיוון ש־$F_{\mathfrak{P}}/F_{\mathfrak{P},s}$ היא הרחבה אי פרידה טהורה, יש חזקה q של $\mathrm{char}\,K = \mathrm{char}\,E$, כך ש־$\pi\big((yz)^q\big) = \big(\pi(yz)\big)^q \in F_{\mathfrak{P},s}$. נשים לב ש־$(yz)^q \in \mathcal{O}'_{\mathfrak{p}}$ ו־$v_{\mathfrak{P}_j}\big((yz)^q\big) > 0$ לכל $2 \leq j \leq r$. לפי למה 32.12

$$\pi\big(\mathrm{tr}_{F/E}(yz)^q\big) = e \cdot \mathrm{tr}_{F_{\mathfrak{P},s}/E_{\mathfrak{p}}}\left(\pi(yz)^q\right) = 0,$$

כי $e = 0$ ב־$F_{\mathfrak{P}}$. מכאן (6). בכך הוכחה טענה 3.

אם נכפיל את y באיבר $x \in E$ כך ש־$v_{\mathfrak{p}}(x) = -1$ (ולכן $v_{\mathfrak{P}_i}(x) = -e_i$ לכל i), נקבל

טענה 4: *יש* $y' \in F$ *כך שלכל* $z \in \mathcal{O}'_{\mathfrak{p}}$

$$v_{\mathfrak{P}}(y') = -e,\ v_{\mathfrak{P}}(y'z) \geq -e \tag{4'}$$

$$v_{\mathfrak{P}_i}(y') > -e_i \quad 2 \leq i \leq r \tag{5'}$$

$$v_{\mathfrak{p}}\big(\operatorname{tr}_{F/E}(y'z)\big) \geq 0 \tag{6'}$$

לפי $(6')$, $y' \in \mathcal{C}_{\mathfrak{p}}$. לכן לפי הערה 32.11(ג) ולפי $(4')$, $-e = v_{\mathfrak{P}}(y') \geq -d(\mathfrak{P}/\mathfrak{p})$. מכאן $d(\mathfrak{P}/\mathfrak{p}) \geq e$.
∎

מסקנה 32.15: *תהי* F/L *הרחבה פרידה סופית של שדה פונקציות* E/K*. אז קבוצת המחלקים הראשוניים של* E *שהינם מסועפים ב־* F *(כלומר, יש מעליהם מחלק ראשוני בעל ציון הסתעפות* > 1*) היא סופית.*

הוכחה: לפי הערה 32.11(ב), $d(\mathfrak{P}/\mathfrak{p}) = 0$ עבור כמעט כל $\mathfrak{p}$ וכל $\mathfrak{P}/\mathfrak{p}$. לכן לפי משפט דדקינד, חלק (א), ($d(\mathfrak{P}/\mathfrak{p}) \geq e(\mathfrak{P}/\mathfrak{p}) - 1$) $e(\mathfrak{P}/\mathfrak{p}) = 1$ עבור כמעט כל $\mathfrak{p}$ וכל $\mathfrak{P}/\mathfrak{p}$. ∎

33. נוסחת רימן־הורביץ

למה 33.1: *תהי L/K הרחבה פרידה סופית. יהי V מרחב וקטורי מעל L ותהי $T\colon V \to K$ העתקה לינארית־K. אז קיימת העתקה לינארית־L יחידה $T'\colon V \to L$ כך שהתרשים הבא חילופי*

$$\begin{tikzcd} V \arrow[r, "T'"] \arrow[d, equal] & L \arrow[d, "\mathrm{tr}_{L/K}"] \\ V \arrow[r, "T"] & K \end{tikzcd}$$

הוכחה: נסמן $n = [L : K]$. אז L מרחב וקטורי בעל מימד n מעל K. לכן המרחב הדואלי

$$L^* = \{t\colon L \to K \mid t \text{ לינארית־} K\}$$

גם מרחב וקטורי בעל מימד n מעל K. (הכפל באברי K מוגדר כך: $(zt)(x) = zt(x)$ עבור $x, z \in K$.)

עבור $t \in L^*$ ו־$z \in L$ נגדיר $z \cdot t \in L^*$ על ידי $(z \cdot t)(x) = t(zx)$. זה הופך את L^* למרחב וקטורי מעל L. צמצום הסקלרים מ־L ל־K מגדיר את המרחב המקורי L^* מעל K, כי עבור $z \in K$ מתקיים $(z \cdot t)(x) = t(zx) = zt(x) = (zt)(x)$. לכן $n = \dim_K L^* = [L : K] \cdot \dim_L L^*$, ומכאן $\dim_L L^* = 1$.

כעת, $0 \neq \mathrm{tr}_{L/K} \in L^*$. לכן לכל $t \in L^*$ יש $z \in L$ יחיד כך ש־$t = z \cdot \mathrm{tr}_{L/K}$.

לכל $v \in V$ נגדיר העתקה $t_v\colon L \to K$ על ידי $t_v(x) = T(xv)$. זוהי הרכבה של העתקה לינארית־L ($x \mapsto xv$) עם העתקה לינארית־K, לכן היא לינארית־K, כלומר, $t_v \in L^*$. לפי הפסקה הקודמת, יש $T'(v) \in L$ יחיד כך ש־$t_v = T'(v) \cdot \mathrm{tr}_{L/K}$. זה מגדיר העתקה $T'\colon V \to L$. היא מקיימת

$$T(xv) = t_v(x) = \big(T'(v) \cdot \mathrm{tr}_{L/K}\big)(x) = \mathrm{tr}_{L/K}\big(T'(v)x\big), \qquad x \in L,\ v \in V \tag{1}$$

טענה: *T' לינארית־L.* אכן, יהיו $v, v_1, v_2 \in V$ ויהי $z \in L$. אז

$$t_{v_1+v_2}(x) = T\big(x(v_1+v_2)\big) = T(xv_1 + xv_2) = T(xv_1) + T(xv_2) = t_{v_1}(x) + t_{v_2}(x)$$

לכל $x \in L$, לכן $t_{v_1+v_2} = t_{v_1} + t_{v_2}$, כלומר, $T'(v_1+v_2) \cdot \mathrm{tr}_{L/K} = T'(v_1) \cdot \mathrm{tr}_{L/K} + T'(v_2) \cdot \mathrm{tr}_{L/K}$. מכאן $T'(v_1+v_2) = T'(v_1) + T'(v_2)$.

באופן דומה

$$t_{zv}(x) = T\big(x(zv)\big) = T\big((zx)v\big) = t_v(zx) = (z \cdot t_v)(x)$$

לכל $x \in L$, לכן $t_{zv} = z \cdot t_v$, כלומר, $T'(zv) \cdot \mathrm{tr}_{L/K} = z \cdot \big(T'(v) \cdot \mathrm{tr}_{L/K}\big) = \big(zT'(v)\big) \cdot \mathrm{tr}_{L/K}$. מכאן $T'(zv) = zT'(v)$.

בכך הוכחה הטענה.

נציב $x = 1$ במשוואה (1). אז $T(v) = \mathrm{tr}_{L/K}\left(T'(v)\right)$ לכל $v \in V$. מכאן $T = \mathrm{tr}_{L/K} \circ T'$.

יחידות: אם גם $T''\colon V \to L$ העתקה לינארית־L כך ש־$T = \mathrm{tr}_{L/K} \circ T''$, אז לכל $x \in L, v \in V$

$$t_v(x) = T(xv) = \mathrm{tr}_{L/K}\left(T''(xv)\right) = \mathrm{tr}_{L/K}\left(xT''(v)\right) = \left(T''(v) \cdot \mathrm{tr}_{L/K}\right)(x)$$

כלומר, $t_v = T''(v) \cdot \mathrm{tr}_{L/K}$ לכל $v \in V$. לפי היחידות של $T'(v)$ נקבל $T''(v) = T'(v)$, לכן $T'' = T'$.

∎

תהי F/L הרחבת שדות פונקציות סופית פרידה של E/K. (כלומר, F/E הרחבה סופית פרידה.)

תזכורת 33.2: (א) **אדל** של F/L הוא פונקציה $\alpha\colon \mathbb{P}(F/L) \to F$ ($\mathfrak{P} \mapsto \alpha_{\mathfrak{P}}$) כך ש־$v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}) \geq 0$ עבור כמעט כל $\mathfrak{P} \in \mathbb{P}$. קבוצת כל האדלים $\mathbb{A}_F$ של F/L היא אלגברה (קומוטטיבית) מעל F ביחס לפעולת לפי הרכיבים ו־$F \to \mathbb{A}_F$ נתונה על ידי $z \mapsto [z]$, באשר $[z]_{\mathfrak{P}} = z$ לכל $\mathfrak{P}$.

לכל מחלק $\mathfrak{D} \in \mathcal{D}(F/L)$ הגדרנו $\Lambda(\mathfrak{D}) = \{\alpha \in \mathbb{A}_F |\ v_{\mathfrak{P}}(\alpha)+v_{\mathfrak{P}}(\mathfrak{D}) \geq 0$ לכל $\mathfrak{P} \in \mathbb{P}(F/L)\}$.

(לפעמים נכתוב גם $\Lambda_F(\mathfrak{D})$ במקום $\Lambda(\mathfrak{D})$. ∎

הגדרה 33.3: (א) $\mathbb{A}_{F/E} = \{\alpha \in \mathbb{A}_F |\ \alpha_{\mathfrak{P}_1} = \alpha_{\mathfrak{P}_2} \Leftarrow \mathfrak{P}_1 \cap E = \mathfrak{P}_2 \cap E\}$. זוהי תת אלגברה (מעל F) של $\mathbb{A}_F$ שמכילה את F.

(ב) עבור מחלק $\mathfrak{D} \in \mathcal{D}(F/L)$ נגדיר

$$\Lambda_{F/E}(\mathfrak{D}) = \mathbb{A}_{F/E} \cap \Lambda(\mathfrak{D}).$$

זהו מרחב וקטורי מעל L.

(ג) נרחיב את העקבה $\mathrm{tr}_{F/E} : F \to E$ להעתקה $\mathrm{tr}_{F/E} : \mathbb{A}_{F/E} \to \mathbb{A}_E$ על ידי $\left(\mathrm{tr}_{F/E}(\alpha)\right)_{\mathfrak{p}} = \mathrm{tr}_{F/E}(\alpha_{\mathfrak{P}})$, לכל $\alpha \in \mathbb{A}_{F/E}$, כאשר $\mathfrak{P}$ מחלק ראשוני כלשהו מעל $\mathfrak{p}$. ∎

הערה 33.4: הגדרה 33.3(ג) היא טובה, כלומר, אם $\alpha \in \mathbb{A}_{F/E}$, אז הפונקציה $\mathrm{tr}_{F/E}(\alpha)\colon \mathbb{P}(E/K) \to E$ היא אדל.

אכן, כמעט לכל $\mathfrak{P} \in \mathbb{P}(F/L)$ מתקיים $v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}) \geq 0$, כלומר, $\alpha_{\mathfrak{P}} \in \mathcal{O}_{\mathfrak{P}}$. לכן עבור כמעט לכל $\mathfrak{p} \in \mathbb{P}(E/K)$ כל $\mathfrak{P} \in \mathbb{P}(F/L)$ מעל $\mathfrak{p}$ הוא כנ"ל, ולכן $\alpha_{\mathfrak{P}}$ (שאינו תלוי ב־$\mathfrak{P}$ אלא רק ב־$\mathfrak{p}$) שייך ל־$\bigcap_{\mathfrak{P}/\mathfrak{p}} \mathcal{O}_{\mathfrak{P}} = \mathcal{O}'_{\mathfrak{p}}$, לפי משפט 32.7(א). לפי תזכורת 32.6(א), $\mathrm{tr}_{F/E}(\alpha_{\mathfrak{P}}) \in \mathcal{O}_{\mathfrak{p}}$.

(ב) אם $z \in F$ אז $\mathrm{tr}_{F/E}[z] = [\mathrm{tr}_{F/E}(z)]$. ∎

למה 33.5: *יהי $\mathfrak{D} \in \mathcal{D}(F/L)$. אז* $\mathbb{A}_F = \mathbb{A}_{F/E} + \Lambda(\mathfrak{D})$.

הוכחה: יהי $\alpha \in \mathbb{A}_F$ אדל. יהי $\mathfrak{p} \in \mathbb{P}(E/K)$. קבוצת המחלקים הראשוניים של F/L מעל $\mathfrak{p}$ היא סופית. לפי משפט הקירוב החלש (משפט 5.10) קיים $x_{\mathfrak{p}} \in F$ כך ש־

$$v_{\mathfrak{P}}(\alpha_{\mathfrak{P}} - x_{\mathfrak{p}}) \geq -v_{\mathfrak{P}}(\mathfrak{D}) \quad \text{לכל } \mathfrak{P}/\mathfrak{p}.$$

כמעט לכל $\mathfrak{p}$ ולכל $\mathfrak{P}/\mathfrak{p}$ מתקיים $v_{\mathfrak{P}}(\mathfrak{D}) = 0$ ו־ $v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}) \geq 0$. אז, בהכרח, $v_{\mathfrak{P}}(x_{\mathfrak{p}}) \geq 0$.

נגדיר $\beta\colon \mathbb{P}(F/L) \to F$ על ידי $\beta_{\mathfrak{P}} = x_{\mathfrak{p}}$, אם $\mathfrak{P}/\mathfrak{p}$. אז $\beta \in \mathbb{A}_{F/E}$ ו־$\alpha - \beta \in \Lambda(\mathfrak{D})$. לכן $\alpha = \beta + (\alpha - \beta) \in \mathbb{A}_{F/E} + \Lambda(\mathfrak{D})$. ∎

תזכורת 33.6:

(א) דיפרנציאל של F/L היא העתקה $\omega\colon \mathbb{A}_F \to L$ לינארית־L שמתאפסת על תת מרחב מהצורה $\Lambda(\mathfrak{D}) + F$.

(ב) לכל דיפרנציאל $\omega \neq 0$ הגדרנו מחלק $(\omega) = \max\{\mathfrak{D} \in \mathcal{D}(F/L) |\ \Lambda(\mathfrak{D}) + F \text{ מתאפס על } \omega\}$.

בפרט ω מתאפס על $\Lambda\big((\omega)\big)$. ∎

למה 33.7: *יהי ω דיפרנציאל על E/K. נגדיר העתקה $\omega_1\colon \mathbb{A}_{F/E} \to K$ על ידי $\omega_1 = \omega \circ \mathrm{tr}_{F/E}$. יהי $\mathfrak{D} = \mathrm{Con}_{F/E}(\omega) + \mathrm{Diff}(F/E) \in \mathcal{D}(F/L)$. אז*

(א) *ω_1 לינארית־ K;*

(ב) *ω_1 מתאפסת על $\Lambda_{F/E}(\mathfrak{D}) + F$;*

(ג) *אם $\mathfrak{D}' \in \mathcal{D}(F)$ מחלק כך ש־ $\mathfrak{D}' \not\leq \mathfrak{D}$, אז יש אדל $\beta \in \Lambda_{F/E}(\mathfrak{D}')$ כך ש־ $\omega_1(\beta) \neq 0$.*

הוכחה: (א) ω_1 היא הרכבה של שתי העתקות לינאריות־K.

(ב) ω_1 מתאפסת על F, כי $\mathrm{tr}_{F/E}(F) \subseteq E$ ו־ω מתאפס על E.

יהי $\alpha \in \Lambda_{F/E}(\mathfrak{D})$. צריך להוכיח ש־$\omega$ מתאפס על $\mathrm{tr}_{F/E}(\alpha)$. כיוון ש־$\omega$ מתאפס על $\Lambda_E\big((\omega)\big)$, די להוכיח כי $\mathrm{tr}_{F/E}(\alpha) \in \Lambda_E\big((\omega)\big)$. כלומר, שלכל $\mathfrak{p} \in \mathbb{P}(E/K)$ מתקיים $v_{\mathfrak{p}}\big(\mathrm{tr}_{F/E}(\alpha)\big) + v_{\mathfrak{p}}\big((\omega)\big) \geq 0$. לכן די להוכיח שלכל $\mathfrak{p} \in \mathbb{P}(E/K)$ ולכל $\mathfrak{P}/\mathfrak{p}$ מתקיים

$$v_{\mathfrak{p}}\big(\mathrm{tr}_{F/E}(\alpha_{\mathfrak{P}})\big) + v_{\mathfrak{p}}\big((\omega)\big) \geq 0. \tag{2}$$

נקבע $\mathfrak{p}$. נבחר $x \in E$ כך ש־ $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}\big((\omega)\big)$. אז לכל $\mathfrak{P}/\mathfrak{p}$

$$\begin{aligned} v_{\mathfrak{P}}(x\alpha_{\mathfrak{P}}) &= v_{\mathfrak{P}}(x) + v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}) \geq e(\mathfrak{P}/\mathfrak{p}) v_{\mathfrak{p}}\big((\omega)\big) - v_{\mathfrak{P}}(\mathfrak{D}) = \\ &= v_{\mathfrak{P}}\big(\mathrm{Con}_{F/E}(\omega) - \mathfrak{D}\big) = v_{\mathfrak{P}}\big(-\mathrm{Diff}(F/E)\big) = -d(\mathfrak{P}/\mathfrak{p}) \end{aligned}$$

לפי הערה 32.11(ג), $x\alpha_{\mathfrak{P}} \in \mathcal{C}_{\mathfrak{p}}$, ולכן, לפי הגדרת $\mathcal{C}_{\mathfrak{p}}$, $v_{\mathfrak{p}}\big(\mathrm{tr}_{F/E}(x\alpha_{\mathfrak{P}})\big) \geq 0$. אבל $\mathrm{tr}_{F/E}$ היא לינארית־E ו־$x \in E$, לכן

$$\begin{aligned} v_{\mathfrak{p}}\big(\mathrm{tr}_{F/E}(x\alpha_{\mathfrak{P}})\big) &= v_{\mathfrak{p}}\big(x\,\mathrm{tr}_{F/E}(\alpha_{\mathfrak{P}})\big) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}\big(\mathrm{tr}_{F/E}(\alpha_{\mathfrak{P}})\big) = \\ &= v_{\mathfrak{p}}\big((\omega)\big) + v_{\mathfrak{p}}\big(\mathrm{tr}_{F/E}(\alpha_{\mathfrak{P}})\big) \end{aligned}$$

ומכאן (2).

(ג) לפי ההנחה יש $\mathfrak{P}' \in \mathbb{P}(F/L)$ כך ש־$v_{\mathfrak{P}'}(\mathfrak{D}') > v_{\mathfrak{P}'}(\mathfrak{D})$. יהי $\mathfrak{p}$ המחלק הראשוני מתחת ל־$\mathfrak{P}'$. אז

$$v_{\mathfrak{P}'}(\mathfrak{D}') > v_{\mathfrak{P}'}(\mathfrak{D}) = v_{\mathfrak{P}'}\big(\mathrm{Con}_{F/E}(\omega)\big) + d(\mathfrak{P}'/\mathfrak{p}).$$

במלים אחרות,

$$v_{\mathfrak{P}'}\big(\operatorname{Con}_{F/E}(\omega)-\mathfrak{D}'\big) < -d(\mathfrak{P}'/\mathfrak{p}). \tag{3}$$

יהי $\mathcal{O}'_{\mathfrak{p}}$ הסגור השלם של $\mathcal{O}_{\mathfrak{p}}$ ב־F, ויהי $\mathcal{C}_{\mathfrak{p}}$ המודול המשלים מעל $\mathcal{O}_{\mathfrak{p}}$. נסמן

$$J := \{z\in F \mid \mathfrak{P}/\mathfrak{p} \text{ לכל } v_{\mathfrak{P}}(z)\ge v_{\mathfrak{P}}\big(\operatorname{Con}_{F/E}(\omega)-\mathfrak{D}'\big)\}.$$

קל לראות ש־J הוא מודול־$\mathcal{O}'_{\mathfrak{p}}$ ו־$\operatorname{tr}_{F/E}(J)$ הוא מודול־$\mathcal{O}_{\mathfrak{p}}$. לפי משפט הקירוב החלש יש $z'\in J$ כך ש־$v_{\mathfrak{P}}(z') = v_{\mathfrak{P}}\big(\operatorname{Con}_{F/E}(\omega)-\mathfrak{D}'\big)$ לכל $\mathfrak{P}$ מעל $\mathfrak{p}$. לפי (3), $v_{\mathfrak{P}'}(z') < -d(\mathfrak{P}'/\mathfrak{p})$. לכן לפי הערה 33.11(ג), $z'\notin \mathcal{C}_{\mathfrak{p}}$. לכן יש $v\in\mathcal{O}'_{\mathfrak{p}}$ כך ש־$\operatorname{tr}_{F/E}(vz')\notin\mathcal{O}_{\mathfrak{p}}$. כיוון ש־$J$ הוא מודול־$\mathcal{O}'_{\mathfrak{p}}$, $vz'\in J$. לכן $\operatorname{tr}_{F/E}(J)\not\subseteq\mathcal{O}_{\mathfrak{p}}$. בפרט $\operatorname{tr}_{F/E}(J)\ne\{0\}$.

נבחר $t\in E$ כך ש־$v_{\mathfrak{p}}(t)=1$. עבור $r\in\mathbb{N}$ גדול מספיק, $t^rJ\subseteq\bigcap_{\mathfrak{P}/\mathfrak{p}}\mathcal{O}_{\mathfrak{P}}=\mathcal{O}'_{\mathfrak{p}}$, לכן $t^r\operatorname{tr}_{F/E}(J)=\operatorname{tr}_{F/E}(t^rJ)\subseteq\mathcal{O}_{\mathfrak{p}}$, לפי תזכורת 32.6(א). לכן $-r\le v_{\mathfrak{p}}\big(\operatorname{tr}_{F/E}(J)\big)$. לפי משפט 32.7(ג) יש $m\in\mathbb{Z}$ כך ש־

$$\operatorname{tr}_{F/E}(J)=t^m\mathcal{O}_{\mathfrak{p}}\,. \tag{4}$$

כיוון ש־$\operatorname{tr}_{F/E}(J)\not\subseteq\mathcal{O}_{\mathfrak{p}}$, מתקיים $m\le -1$.

כזכור, (ω) הוא המחלק הגדול ביותר ב־$\mathcal{D}(E/K)$ כך ש־ω מתאפס על $\Lambda_E\big((\omega)\big)$ (וגם על E). כיוון ש־$(\omega)+\mathfrak{p} < (\omega)$, יש $\alpha\in\Lambda_E\big((\omega)+\mathfrak{p}\big)$ כך ש־$\omega(\alpha)\ne 0$. כיוון ש־ω כן מתאפס על $\Lambda_E\big((\omega)\big)$, בהכרח $\alpha\notin\Lambda_E\big((\omega)\big)$. אז $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})\ge -v_{\mathfrak{p}}\big((\omega)\big)-1$, אבל $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})\not\ge -v_{\mathfrak{p}}\big((\omega)\big)$, לכן

$$v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = -v_{\mathfrak{p}}\big((\omega)\big)-1. \tag{5}$$

יהיו $\gamma,\gamma'\in\mathbb{A}_E$ נתונים על ידי

$$\gamma_{\mathfrak{q}}=\begin{cases}\alpha_{\mathfrak{p}} & \mathfrak{q}=\mathfrak{p}\\ 0 & \mathfrak{q}\ne\mathfrak{p}\end{cases},\quad \gamma'_{\mathfrak{q}}=\begin{cases}0 & \mathfrak{q}=\mathfrak{p}\\ \alpha_{\mathfrak{q}} & \mathfrak{q}\ne\mathfrak{p}\end{cases}.$$

אז $\gamma=\alpha-\gamma'$, ו־$\gamma'\in\Lambda_E\big((\omega)\big)$, לכן $\omega(\gamma')=0$. מכאן $\omega(\gamma)=\omega(\alpha)-\omega(\gamma')\ne 0$.

נסמן $x=\gamma_{\mathfrak{p}}=\alpha_{\mathfrak{p}}$.

נבחר $y\in E$ כך ש־$v_{\mathfrak{p}}(y)=v_{\mathfrak{p}}\big((\omega)\big)$, אז, לפי (5), $v_{\mathfrak{p}}(xy)=v_{\mathfrak{p}}(x)+v_{\mathfrak{p}}(y)=-1\ge m$, לכן $xy\in t^m\mathcal{O}_{\mathfrak{p}}$. לפי (4)

$$\text{יש } z\in J \text{ כך ש־} \operatorname{tr}_{F/E}(z)=xy\,.$$

נגדיר אדל $\beta\in\mathbb{A}_{F/E}$ על ידי

$$\beta_{\mathfrak{P}}=\begin{cases} zy^{-1} & \mathfrak{P}/\mathfrak{p}\\ 0 & \text{אחרת}\end{cases}.$$

אז לפי ההגדרה של J, אם $\mathfrak{P}/\mathfrak{p}$, אז $v_{\mathfrak{P}}(z) \geq v_{\mathfrak{P}}\big(\operatorname{Con}_{F/E}((\omega)) - \mathfrak{D}'\big)$, ולכן

$$v_{\mathfrak{P}}(\beta) = v_{\mathfrak{P}}(z) - v_{\mathfrak{P}}(y) \geq v_{\mathfrak{P}}\big(\operatorname{Con}_{F/E}((\omega)) - \mathfrak{D}'\big) - v_{\mathfrak{P}}\big(\operatorname{Con}_{F/E}((\omega))\big) = -v_{\mathfrak{P}}(\mathfrak{D}').$$

ואם $\mathfrak{P}$ אינו מונח מעל $\mathfrak{p}$, אז $v_{\mathfrak{P}}(\beta) = v_{\mathfrak{P}}(0) = \infty \geq -v_{\mathfrak{P}}(\mathfrak{D}')$. לכן $\beta \in \Lambda_{F/E}(\mathfrak{D}')$. נשים לב ש־$\operatorname{tr}_{F/E}(\beta) = \gamma$, כי

$$\big(\operatorname{tr}_{F/E}(\beta)\big)_{\mathfrak{q}} = \begin{cases} \operatorname{tr}_{F/E}(zy^{-1}) = y^{-1}\operatorname{tr}_{F/E}(z) = y^{-1}yx = \gamma_{\mathfrak{q}} & \mathfrak{q} = \mathfrak{p} \\ \operatorname{tr}_{F/E}(0) = 0 = \gamma_{\mathfrak{q}} & \text{אחרת} \end{cases} = \gamma_{\mathfrak{q}}$$

לכן $\omega_1(\beta) = \omega\big(\operatorname{tr}_{F/E}(\beta)\big) = \omega(\gamma) \neq 0$, לפי (5). ∎

משפט 33.8: *לכל דיפרנציאל ω של E/K קיים דיפרנציאל יחיד ω' של F/L שמקיים*

$$\operatorname{tr}_{L/K}\big(\omega'(\beta)\big) = \omega(\big(\operatorname{tr}_{F/E}(\beta)\big), \qquad \beta \in \mathbb{A}_{F/E}.$$

אם $\omega \neq 0$ אז $\omega' \neq 0$ ו־$(\omega') = \operatorname{Con}_{F/E}\big((\omega)\big) + \operatorname{Diff}(F/E)$.

הוכחה: יהי $\mathfrak{D} = \operatorname{Con}_{F/E}(\omega) + \operatorname{Diff}(F/E) \in \mathcal{D}(F/L)$. נגדיר העתקה $\omega_1 \colon \mathbb{A}_{F/E} \to K$ על ידי $\omega_1 = \omega \circ \operatorname{tr}_{F/E}$ (כמו בלמה 33.7).

נרחיב את ω_1 להעתקה $\omega_2 \colon \mathbb{A}_F \to K$ על ידי $\omega_2(\beta + \gamma) = \omega_1(\beta)$, באשר $\gamma \in \Lambda_F(\mathfrak{D})$ ו־$\beta \in \mathbb{A}_{F/E}$.

ההגדרה טובה: לפי למה 33.5, $\mathbb{A}_F = \mathbb{A}_{F/E} + \Lambda_F(\mathfrak{D})$, לכן כל אדל $\alpha \in \mathbb{A}_F$ הוא מהצורה $\alpha = \beta + \gamma$, עם β, γ כמו לעיל. אם $\alpha = \beta_1 + \gamma_1 = \beta_2 + \gamma_2$, באשר $\gamma_1, \gamma_2 \in \Lambda_F(\mathfrak{D})$, ו־$\beta_1, \beta_2 \in \mathbb{A}_{F/E}$. אז

$$\beta_1 - \beta_2 = \gamma_2 - \gamma_1 \in \mathbb{A}_{F/E} \cap \Lambda(\mathfrak{D}) = \Lambda_{F/E}(\mathfrak{D}),$$

לכן $\omega_1(\beta_1) - \omega_1(\beta_2) = \omega_1(\beta_1 - \beta_2) = 0$ לפי למה 33.7(א), (ב).

ברור ש־ω_2 היא לינארית־K. לכן לפי למה 33.1 קיימת העתקה לינארית־L יחידה $\omega' \colon \mathbb{A}_F \to L$ כך ש־$\omega_2 = \operatorname{tr}_{L/K} \circ \omega'$. מההגדרות של ω_1, ω_2 נקבל

$$\operatorname{tr}_{L/K}\big(\omega'(\beta)\big) = \omega_2(\beta + 0) = \omega_1(\beta) = \omega\big(\operatorname{tr}_{F/E}(\beta)\big), \qquad \beta \in \mathbb{A}_{F/E},$$

כמבוקש.

נראה ש־ω' הוא דיפרנציאל. ביתר דיוק, נראה:

טענה 1: *ω' מתאפס על $F + \Lambda(\mathfrak{D})$.* אם לא, אז כיוון ש־$\omega'$ היא העתקה לינארית־L לתוך L, מתקיים $\omega'\big(\Lambda(\mathfrak{D}) + F\big) = L$. כיוון ש־$\operatorname{tr}_{L/K}$ היא על, $\operatorname{tr}_{L/K}\big(\omega'(\Lambda(\mathfrak{D}) + F)\big) = K$. אבל $\omega_2 = \operatorname{tr}_{L/K} \circ \omega'$ מרחיבה את ω_1, וזו מתאפסת על $\Lambda(\mathfrak{D}) + F$, לפי למה 33.7(ב). סתירה.

טענה 2: *ω' הוא יחיד.* נניח שגם ω'' הוא דיפרנציאל של F/L שמקיים גם הוא

$$\operatorname{tr}_{L/K}\left(\omega''(\beta)\right) = \operatorname{tr}_{L/K}\left(\omega'(\beta)\right) = \omega\big(\operatorname{tr}_{F/E}(\beta)\big), \qquad \beta \in \mathbb{A}_{F/E}\ .$$

יהי $\eta = \omega'' - \omega'$. זהו דיפרנציאל של F/L, ובפרט העתקה לינארית־L, שמקיימת $\operatorname{tr}_{L/K}\left(\eta(\beta)\right) = 0$ לכל $\beta \in \mathbb{A}_{F/E}$. לכן $\eta(\mathbb{A}_{F/E}) \subsetneqq L$, ולכן $\eta(\mathbb{A}_{F/E}) = 0$. כיוון ש־$\eta$ הוא דיפרנציאל, הוא מתאפס גם על $\Lambda_F(\mathfrak{D}')$ עבור איזה מחלק $\mathfrak{D}' \in \mathcal{D}(F/L)$. לפי למה 33.5, η מתאפס על $\mathbb{A}_F$, כלומר, $\eta = 0$. מכאן $\omega'' = \omega'$.

לבסוף, אם $\mathfrak{D}' \in \mathcal{D}(F/L)$ מחלק שמקיים $\mathfrak{D} \not\leq \mathfrak{D}'$, אז ω' אינו מתאפס על $\Lambda_F(\mathfrak{D}')$, כי לפי למה 33.7(ג) יש אדל $\beta \in \Lambda_{F/E}(\mathfrak{D}') \subseteq \Lambda_F(\mathfrak{D}')$ כך ש־$\omega_2(\beta) = \omega_1(\beta) \neq 0$; מכאן $\omega'(\beta) \neq 0$.

זה, יחד עם טענה 1, נותן ש־$\mathfrak{D}$ הוא המחלק המרבי כך ש־ω' מתאפס על $\Lambda(\mathfrak{D}) + F$, כלומר, $(\omega') = \mathfrak{D} = \operatorname{Con}_{F/E}\left((\omega)\right) + \operatorname{Diff}(F/E)$. ∎

הגדרה 33.9: ההעתקה $\omega \mapsto \omega'$, באשר ω' כמו במשפט 33.8, נקראת **קו־עקבה** ותסומן $\operatorname{cotr}_{F/E}$. היא מוגדרת, באופן לא מפורש, על יד המשוואה $\operatorname{tr}_{L/K} \circ \operatorname{cotr}_{F/E}(\omega) = \omega \circ \operatorname{tr}_{F/E}$ על $\mathbb{A}_{F/E}$. ∎

תרגיל 33.10: *(א) יהיו* $\omega_1, \omega_2 \in \Omega_{E/K}$. *אז* $\operatorname{cotr}_{F/E}(\omega_1 + \omega_2) = \operatorname{cotr}_{F/E}(\omega_1) + \operatorname{cotr}(\omega_2)$.

(ב) *יהי* $\omega \in \Omega_{E/K}$ *ויהי* $x \in E$. *אז* $\operatorname{cotr}_{F/E}(x\omega) = x\operatorname{cotr}(\omega)$.

(ג) *תהיינה* $F/E,\, F'/F$ *הרחבות פרידות סופיות של שדות פונקציות. אז* $\operatorname{cotr}_{F'/E} = \operatorname{cotr}_{F'/F} \circ \operatorname{cotr}_{F/E}$.

הוכחה: על $\mathbb{A}_{F/E}$ מתקיים

$$\operatorname{tr}_{L/K} \circ \operatorname{cotr}_{F/E}(\omega_1) = \omega_1 \circ \operatorname{tr}_{F/E}$$

$$\operatorname{tr}_{L/K} \circ \operatorname{cotr}_{F/E}(\omega_2) = \omega_2 \circ \operatorname{tr}_{F/E}$$

נחבר את שתי המשוואות; כיוון ש־$\operatorname{tr}_{L/K}$ לינארית־K, נקבל

$$\operatorname{tr}_{L/K} \circ \big(\operatorname{cotr}_{F/E}(\omega_1) + \operatorname{cotr}_{F/E}(\omega_1)\big) = (\omega_1 + \omega_2) \circ \operatorname{tr}_{F/E}$$

ומכאן, לפי ההגדרה הלא מפורשת של cotr, נובע (א).

(ב) לפי ההגדרה של cotr מתקיים $\operatorname{tr}_{L/K} \circ \operatorname{cotr}_{F/E}(\omega) \circ [x] = \omega \circ \operatorname{tr}_{F/E} \circ [x]$ על $\mathbb{A}_{F/E}$ (כאשר $[x]$ מסמן את הכפלה ב־x). כיוון ש־$x \in E$, מתקיים $[x] \circ \operatorname{tr}_{F/E} = \operatorname{tr}_{F/E} \circ [x]$. לפי ההגדרה של הכפל של דיפרנציאלים בסקלר (תרגיל 11.1), $x\omega = \omega \circ [x]$ ו־$\operatorname{cotr}_{F/E}(\omega) \circ [x] = \big(x\operatorname{cotr}_{F/E}(\omega)\big)$. לכן

$$\operatorname{tr}_{L/K} \circ \big(x\operatorname{cotr}_{F/E}(\omega)\big) = (x\omega) \circ \operatorname{tr}_{F/E}$$

וזה, לפי ההגדרה הלא מפורשת, נותן את (ב).

(ג) יהיו $K \subseteq L \subseteq L'$ שדות הקבועים של $E \subseteq F \subseteq F'$. יהי $\omega \in \Omega_{E/K}$. אז

$$\operatorname{tr}_{L'/K} \circ \big(\operatorname{cotr}_{F'/F} \circ \operatorname{cotr}_{F/E}\big)(\omega) = \operatorname{tr}_{L/K} \circ \big(\operatorname{tr}_{L'/L} \circ \operatorname{cotr}_{F'/F}\big) \circ \operatorname{cotr}_{F/E}(\omega) =$$
$$\operatorname{tr}_{L/K} \circ \big(\operatorname{cotr}_{F/E}(\omega) \circ \operatorname{tr}_{F'/F}\big) = \omega \circ \operatorname{tr}_{F/E} \circ \operatorname{tr}_{F'/F} = \omega \circ \operatorname{tr}_{F'/E}$$

∎

משפט 33.11 (נוסחת רימן־הורביץ): *תהי F/L הרחבה פרידה סופית של שדה פונקציות E/K. יהיו g_E, g_F הגזעים של E, F, בהתאמה. אז*

$$.2g_F - 2 = \frac{[F:E]}{[L:K]}(2g_E - 2) + \deg \mathrm{Diff}(F/E)$$

הוכחה: יהי $0 \neq \omega \in \Omega_{E/K}$. לפי משפט 33.8,

$$.\big(\mathrm{cotr}(\omega)\big) = \mathrm{Con}_{F/E}\left((\omega)\right) + \mathrm{Diff}(F/E)$$

כעת, (ω) הוא מחלק קנוני של E/K ו־$\big(\mathrm{cotr}(\omega)\big)$ הוא מחלק קנוני של F/L (הגדרה 11.11). לפי מסקנה 12.2(ב), $\deg_E(\omega) = 2g_E - 2$. ו־$\deg_F\big(\mathrm{cotr}_{F/E}(\omega)\big) = 2g_F - 2$. לפי למה 21.2(ו), $\deg_F \mathrm{Con}_{F/E}\left((\omega)\right) = \frac{[F:E]}{[L:K]}\deg_E(\omega)$. מכאן המסקנה. ∎

מסקנה 33.12: *תהי F/L הרחבה פרידה סופית של שדה פונקציות E/K. יהיו g_E, g_F הגזעים של E, F, בהתאמה. אז $g_E \leq g_F$.*

הוכחה: לפי תרגיל 21.4, $\frac{[F:E]}{[L:K]} \geq 1$. כמו כן $\mathrm{Diff}(F/E) \geq 0$. לכן

$$2g_F - 2 = \frac{[F:E]}{[L:K]}(2g_E - 2) + \deg \mathrm{Diff}(F/E) \geq 2g_E - 2$$

ומכאן המסקנה. ∎

מסקנה 33.13 (Hurwitz): *יהי F שדה פונקציות מעל שדה סגור אלגברית K בעל גזע $g \geq 2$. תהי $G \leq \mathrm{Aut}(F/K)$ חבורה סופית של אוטומורפיזמים של F מעל K. נניח ש־$\mathrm{char}\, K$ זר לסדר של G. אז $|G| \leq 84(g-1)$.*

הוכחה: יהי E שדה השבת של G. אז F/E הרחבת גלואה סופית, $[F:E] = |G|$. כיוון ש־F/K אינה הרבחה אלגברית, ואילו F/E אלגברית, E/K אינה אלגברית, ולכן יש $t \in E$ טרנסצנדנטי מעל K. כמו כן $[E:K(t)] \leq [F:K(t)] < \infty$ ו־K שדה סגור אלגברית. לכן E/K הוא שדה פונקציות אלגבריות במשתנה אחד עם שדה הקבועים K.

לפי מסקנה 32.15 יש רק מספר סופי של מחלקים ראשוניים של E מסועפים ב־F. יהיו $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ כל המחלקים האלה ($k \geq 0$), כאשר מעל $\mathfrak{p}_i$ יש r_i מחלקים ראשוניים של F, כל אחד מהם בעל ציון ההסתעפות e_i. ציון השארית של מחלק $\mathfrak{P}$ מעל $\mathfrak{p}_i$ הוא $f_i = 1$ ו־$\deg \mathfrak{P} = 1$, כי K סגור אלגברית.

לפי מסקנה 20.11(ב), $[F:E] = e_i f_i r_i$, לכן $r_i = \frac{|G|}{e_i}$. לפי משפט הדיפרנט של דדקינד, $d(\mathfrak{P}/\mathfrak{p}_i) = e_i - 1$ לכל $\mathfrak{P}$ מעל $\mathfrak{p}_i$. כל זה נכון גם למחלק ראשוני $\mathfrak{p}$ של E בעל ציון הסתעפות $e = 1$, בפרט, $d(\mathfrak{P}/\mathfrak{p}) = 0$ לכל $\mathfrak{P}$ מעל $\mathfrak{p}$ כזה. לכן $\mathrm{Diff}(F/E) = \sum_{i=1}^k \sum_{\mathfrak{P}/\mathfrak{p}_i}(e_i - 1)\mathfrak{P}$. מכאן

$$.\deg \mathrm{Diff}(F/E) = \sum_{i=1}^k r_i(e_i - 1) = \sum_{i=1}^k \frac{|G|}{e_i}(e_i - 1) = |G|\sum_{i=1}^k(1 - \frac{1}{e_i})$$

לפי נוסחת רימן־הורביץ

$$.2g-2=|G|\cdot\Big(2g_E-2+\sum_{i=1}^{k}(1-\frac{1}{e_i})\Big) \tag{8}$$

נסמן $R=2g_E-2+\sum_{i=1}^{k}(1-\frac{1}{e_i})$, אז $|G|=\frac{2(g-1)}{R}$. לכן די להוכיח: $R\geq\frac{2}{84}=\frac{1}{42}$.

נסמן גם $\lambda_i=1-\frac{1}{e_i}$ לכל $1\leq i\leq k$. אז $\lambda_i\in\{\frac{1}{2},\frac{2}{3},\frac{3}{4},\ldots\}$ ובפרט $\frac{1}{2}\leq\lambda_i<1$. לפי הנתון, $2g-2\geq 2>0$. כמו כן $|G|>0$. לכן $R=\frac{2g-2}{|G|}>0$.

על כן די להוכיח

טענה: *יהי* $k\geq 0$*, יהיו* $\lambda_1,\ldots,\lambda_k\in\{\frac{1}{2},\frac{2}{3},\frac{3}{4},\ldots\}$*, יהי* $g_E\geq 0$ *שלם ויהי* $0<R=2g_E-2+\sum_{i=1}^{k}\lambda_i$. *אז* $R\geq\frac{1}{42}$.

נפריד את ההוכחה למקרים:

(א) אם $g_E\geq 2$, אז $R\geq 2g_E-2\geq 2$.

(ב) אם $g_E=1$, אז $0<R=\sum_{i=1}^{k}\lambda_i$, לכן $k\geq 1$ ולכן $R\geq\frac{1}{2}$.

(ג) אם $g_E=0$, אז $0<R=-2+\sum_{i=1}^{k}\lambda_i\leq -2+\sum_{i=1}^{k}1=-2+k$, לכן $k\geq 3$.

(ג1) אם $k\geq 5$, אז $R=-2+\sum_{i=1}^{k}\lambda_i\geq -2+k\cdot\frac{1}{2}\geq -2+\frac{5}{2}=\frac{1}{2}$.

(ג2) אם $k=4$, אז לא יתכן ש־$\lambda_1=\ldots=\lambda_4=\frac{1}{2}$, כי $R>0$, לכן

$R=-2+\sum_{i=1}^{k}\lambda_i\geq -2+3\cdot\frac{1}{2}+\frac{2}{3}=\frac{1}{6}$.

(ג3) נשאר המקרה $k=3$, כלומר, $R=\lambda_1+\lambda_2+\lambda_3-2$. בלי הגבלת הכלליות $\lambda_1\leq\lambda_2\leq\lambda_3$.

(ג3.1) נניח $\lambda_1>\frac{1}{2}$. לא יתכן ש־$\lambda_1=\lambda_2=\lambda_3=\frac{2}{3}$, כי אז $R=0$. לכן $R\geq\frac{2}{3}+\frac{2}{3}+\frac{3}{4}-2=\frac{1}{12}$.

(ג3.2) נניח $\lambda_1=\frac{1}{2}$. אז לא יתכן שגם $\lambda_2=\frac{1}{2}$, אחרת $R<\frac{1}{2}+\frac{1}{2}+1-2=0$, סתירה.

(ג3.2.1) אם $\lambda_2=\frac{2}{3}$, אז $\lambda_1+\lambda_2-2=-\frac{5}{6}$, לכן כדי ש־$R$ יהיה חיובי, צריך להיות $\lambda_3\geq\frac{6}{7}$ ואז $R\geq-\frac{5}{6}+\frac{6}{7}=\frac{1}{42}$.

(ג3.2.2) אם $\lambda_2=\frac{3}{4}$, אז לא יתכן שגם $\lambda_3=\frac{3}{4}$, אחרת $R=\frac{1}{2}+\frac{3}{4}+\frac{3}{4}-2=0$, סתירה. לכן $R\geq\frac{1}{2}+\frac{3}{4}+\frac{4}{5}-2=\frac{1}{20}$.

(ג3.2.3) אחרת $\lambda_2\geq\frac{4}{5}$, ולכן $R\geq\frac{1}{2}+\frac{4}{5}+\frac{4}{5}-2=\frac{1}{10}$.

בכל המקרים $R\geq\frac{1}{42}$. ∎

מסקנה 33.14: *יהי* E/K *שדה פונקציות בעל גזע* 0. *אזי אין ל־*E *הרחבה פרידה סופית נאותה* F/K *עם אותו שדה קבועים, שאינה מסועפת (כלומר,* $e(\mathfrak{P}/\mathfrak{p})=1$ *לכל* $\mathfrak{p}\in\mathbb{P}_E$ *ולכל* $\mathfrak{P}\in\mathbb{P}_F$ *מעליו).*

הוכחה: נניח שיש. לפי משפט 32.14(ב), $d(\mathfrak{P}/\mathfrak{p})=e(\mathfrak{P}/\mathfrak{p})-1=0$ לכל $\mathfrak{p}\in\mathbb{P}_E$ ולכל $\mathfrak{P}\in\mathbb{P}_F$ מעליו. לכן $\mathrm{Diff}(F/E)=0$. לפי נוסחת רימן־הורביץ

$$.2g_F-2=[F:E](2\cdot 0-2)$$

כלומר, $g_F = 1 - [F:E]$. כיוון ש־$g_F \geq 0$, מכאן $[F:E] = 1$, כלומר, $F = E$. ∎

מסקנה 33.15: *יהי E/K שדה פונקציות בעל גזע 0 מעל שדה סגור אלגברית K. תהי F/K הרחבה סופית שלו, $F \neq E$, מסועפת בריסון ($\operatorname{char} K$ אינו מחלק את ציוני ההסתעפות של הרחבות המחלקים הראשוניים). אז לפחות שני מחלקים ראשוניים שונים של E מסועפים ב־F.*

הוכחה: לפי משפט 32.14(ב), $d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1$. לכן נוסחת רימן־הורביץ נותנת

$$2g_F - 2 = -2[F:E] + \sum_{\mathfrak{p}\in\mathbb{P}(E)} \sum_{\mathfrak{P}/\mathfrak{p}} (e(\mathfrak{P}/\mathfrak{p}) - 1).$$

לפי מסקנה 33.14 יש $\mathfrak{p} \in \mathbb{P}(E)$ מסועף ב־F. נניח בשלילה שהוא יחיד. יהיו $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}(F)$ המחלקים הראשוניים של F מעליו. אז

$$\begin{aligned} -2 \leq 2g_F - 2 &= -2[F:E] + \sum_{i=1}^{r}(e(\mathfrak{P}_i/\mathfrak{p}) - 1) = -2[F:E] + \sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) - r \\ &= -2[F:E] + [F:E] - r = -[F:E] - r \end{aligned}$$

מכאן $[F:E] + r \leq 2$. אבל $[F:E] \geq 2$, לכן $r \leq 0$, סתירה. ∎

מסקנה 33.16: *יהי K שדה סגור אלגברית בעל אפיון $p > 0$. יהי $E = K(t)$ שדה הפונקציות הרציונליות מעל K ויהי $\mathfrak{p} \in \mathbb{P}(E/K)$. תהי F הרחבת גלואה סופית של E כך ש־$\mathfrak{p}$ המחלק הראשוני היחיד של E שהינו מסועף בה. אז $\operatorname{Gal}(F/E)$ הינה חבורה קוואזי־p, דהיינו, היא נוצרת על ידי חבורות סילוב־p שלה.*

הוכחה: כיוון ש־K סגור אלגברית, כל הרחבה סופית של E היא שדה פונקציות אלגבריות במשתנה אחד מעל K.

תהי $G = \operatorname{Gal}(F/E)$ ותהי $P \leq G$ חבורת סילוב־p שלה. תהי $H = \langle P^g |\ g \in G\rangle$ התת חבורה של G הנוצרת על ידי חבורות סילוב־p שלה. ויהי E' שדה השבת שלה בתוך F. כיוון ש־$\{P^g |\ g \in G\}$ סגורה תחת ההצמדה, $\operatorname{Gal}(F/E') = H \triangleleft G$. לכן E'/E הרחבת גלואה.

כיוון ש־$P \leq H \leq G$, המעלה $[E':E] = (G:H)|(G:P)$ זרה ל־p. יהי $\mathfrak{P}$ מחלק ראשוני של E'/K מעל $\mathfrak{p}$. אז לפי מסקנה 20.11(ב), $e(\mathfrak{P}/\mathfrak{p})$ מחלק את $[E':E]$, לכן גם הוא זר ל־p (כלומר, $\mathfrak{p}$ מסועף באופן מרוסן ב־E'). כלומר, p אינו מחלק את ציון ההסתעפות של $\mathfrak{p}$ ב־E'. לפי מסקנה 33.15(ב), $E' = E$. לכן $G = H = \langle P^g |\ g \in G\rangle$ נוצרת על ידי חבורות סילוב־p שלה. ∎

מסקנה 33.17 (Lüroth): *יהי F שדה פונקציות רציונליות מעל שדה K. יהי $K \subsetneqq E \subsetneqq F$ שדה ביניים. אז E הוא שדה פונקציות רציונליות מעל שדה K.*

הוכחה: כיוון ש־K סגור אלגברית ב־F, הוא גם סגור אלגברית ב־E. יש $t \in E \smallsetminus K$. אז $t \in F \smallsetminus K$, לכן t טרנסצנדנטי מעל K, ולכן $[F:K(t)] < \infty$. כיוון ש־$K(t) \subseteq E \subseteq F$, גם $[E:K(t)], [F:E] < \infty$. לכן E/K שדה פונקציות ו־F/E הרחבה סופית.

תחילה נניח ש־F/E פרידה. לפי משפט 14.1, $g_F = 0$. לכן לפי מסקנה 33.12, $g_E = 0$. כמו כן יש ל־F/K מחלק ראשוני $\mathfrak{P}$ ממעלה 1, למשל, זה שמתאים להערכה v_∞ (או לפי משפט 16.2). יהי $\mathfrak{p}$ המחלק הראשוני של E/K מתחת ל־$\mathfrak{P}$, אז $K \subseteq E_\mathfrak{p} \subseteq F_\mathfrak{P} = K$, לכן גם $\mathfrak{p}$ ממעלה 1. לכן E/K שדה פונקציות רציונליות לפי משפט 16.2.

במקרה הכללי יהי E_s הסגור הפריד של E בתוך F. אז E_s/E פרידה סופית, לכן לפי הפסקה הקודמת די להוכיח ש־E_s/K שדה פונקציות רציונליות. כמו כן F/E_s אי פרידה טהורה, לכן בלי הגבלת כלליות F/E אי פרידה טהורה.

יהי $x \in F$ כך ש־$F = K(x)$. אז גם $F = E(x)$ והפולינום האי פריק של x מעל E הוא מהצורה $X^q - a$, באשר q חזקה של $\mathrm{char}\, K$ ו־$a \in E$, לכן $[F : E] = q$. כעת, $K(x^q) \subseteq E \subseteq K(x) = F$, ולכן $[F : K(x^q)] \geq [F : E] = q$, ו־$F = K(x^q)(x)$ אבל $X^q - a$ הוא גם פולינום מעל $K(x^q)$, כי $a = x^q \in K(x^q)$, לכן $[F : K(x^q)] \leq q$. מכאן $[F : K(x^q)] = [F : E]$, ולכן $E = K(x^q)$. לכן E/K שדה פונקציות רציונליות. ∎

מסקנה 33.18 (משפט פרמה לפולינומים): *יהי K שדה ויהי $n \geq 3$ זר ל־$\mathrm{char}\, K$. אז אין קיימים פולינומים $f, g, h \in K[Z]$ שונים מ־0 כך ש־$f^n + g^n = h^n$, אלא אם $f/h, g/h \in K^\times$.*

הוכחה: בלי הגבלת הכלליות K סגור אלגברית.

יהי $n \in \mathbb{N}$. נבחר x טרנסצנדנטי מעל K ונבחר y בסגור האלגברי של $K(x)$ כך ש־$x^n + y^n = 1$. אז $F = K(x, y)$ שדה פונקציות אלגבריות במשתנה אחד מעל K. יהי $\zeta_n \in K$ שורש יחידה n־י פרימיטיבי.

טענה 1: *$[K(x, y) : K(x)] = n$, והמחלקים הראשוניים של $K(x)$ שמתאימים ל־$x - \zeta_n^i$, באשר $0 \leq i < n$, הם מסועפים לגמרי ב־F.* אכן, יהי $\mathfrak{p}$ המחלק הראשוני של $K(x)$ המתאים ל־$x - \zeta_n^i$. אז $v_\mathfrak{p}(x - \zeta_n^i) = 1$ ו־$v_\mathfrak{p}(\zeta_n^j - \zeta_n^i) = 0$ לכל $0 \leq j < n$ שונה מ־i (כי $v_\mathfrak{p}(K^\times) = 0$), לכן

$$v_\mathfrak{p}(x - \zeta_n^j) = v_\mathfrak{p}\big((x - \zeta_n^i) - (\zeta_n^j - \zeta_n^i)\big) = \min(1, 0) = 0$$

מכאן

$$.v_\mathfrak{p}(y^n) = v_\mathfrak{p}(x^n - 1) = v_\mathfrak{p}\Big(\prod_{i=0}^{n-1}(x - \zeta_n^i)\Big) = \sum_{i=0}^{n-1} v_\mathfrak{p}(x - \zeta_n^i) = 1$$

יהי $\mathfrak{P}$ מחלק ראשוני של F מעל ל־$\mathfrak{p}$. אז

$$,nv_\mathfrak{P}(y) = v_\mathfrak{P}(y^n) = e(\mathfrak{P}/\mathfrak{p})v_\mathfrak{p}(y^n) = e(\mathfrak{P}/\mathfrak{p}) \leq [F : K(x)] \leq n$$

לכן $v_\mathfrak{P}(y) = 1$ ומתקיים $e(\mathfrak{P}/\mathfrak{p}) = n = [F : K(x)]$. בכך הוכחה טענה 1. לפי השוויון היסודי (משפט 19.8), $\mathfrak{P}$ הוא המחלק הראשוני היחיד של F מעל $\mathfrak{p}$.

טענה 2: *יהיו $f, g, h \in K[Z]$ שונים מ־0 כך ש־$f^n + g^n = h^n$ ו־$f/h \notin K^\times$. אז F מוכל בשדה פונקציות רציונליות מעל K.*

אכן, נסמן $f_0 = \frac{f}{h}$ ו־$g_0 = \frac{g}{h}$, אז $f_0^n + g_0^n = 1$ ו־$f_0 \in K(Z) \setminus K$. בפרט f_0 טרנסצנדנטי מעל K ולכן העתקת־K $K(x) \to K(Z)$ הנתונה על יד $x \mapsto f_0$ היא איזומורפיזם $K(x) \to K(f_0) \subseteq K(Z)$. לפי טענה 1, $Y^n + x^n - 1 = Y^n - y^n \in K(x)[Y]$ הוא הפולינום האי פריק של y מעל $K(x)$. לכן $Y^n + f_0^n - 1 = Y^n - g_0^n \in K(Z)[Y]$ הוא הפולינום האי פריק של g_0 מעל $K(f_0)$. לכן האיזומורפיזם הנ"ל ניתן להרחבה לאיזומורפיזם־K $F \to K(f_0, g_0) \subseteq K(Z)$.

בכך הוכחה טענה 2. לפי מסקנה 33.17, $g_F = 0$. כמובן, $g_{K(x)} = 0$.

מעל כל אחד מבין n המחלקים $\mathfrak{p}$ של $K(x)$ בטענה 1 יש מחלק ראשוני יחיד $\mathfrak{P}$ של F, ומתקיים $e(\mathfrak{P}/\mathfrak{p}) = n$ ולכן $d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1 = n - 1$ (היחידות נובעת מהשוויון היסודי). לפי נוסחת רימן־הורביץ עבור $F/K(x)$

$$0 - 2 = n(0-2) + n(n-1) + \sum_{\mathfrak{P} \in S} d(\mathfrak{P}/\mathfrak{p}),$$

באשר S היא קבוצת המחלקים הראשוניים של F שמסועפים מעל $K(x)$ ואינם מונחים מעל המחלקים של $K(x)$ שמתוארים בטענה 1. כלומר, $\sum_{\mathfrak{P} \in S} d(\mathfrak{P}/\mathfrak{p}) = -n^2 + 3n - 2 = -(n-1)(n-2)$. אגף שמאל הוא אי שלילי. אם $n \geq 3$, אז אגף ימין הוא שלילי, סתירה. לכן $n = 1$ או $n = 2$ (ו־$S = \emptyset$). ∎

פתרונות תרגילים נבחרים

דוגמאות 1.7: (3) יהי x טרנסצנדנטי מעל שדה F. תהי $w\colon F^\times \to \Gamma$ הערכה. תהי $\Gamma \oplus \mathbb{Z}$ (עם הסדר הלקסיקוגרפי) חבורה סדורה ונגדיר $v\colon F(x)^\times \to \Gamma \oplus \mathbb{Z}$ באופן הבא: אם $0 \neq f = \sum_i a_i x^i \in F[x]$, יהי $v(f) = \min_i \big(w(a_i), i\big)$, ועבור $0 \neq f, g \in F[x]$ נגדיר $v(f/g) = v(f) - v(g)$. אפשר להראות שההגדרה טובה ו־v הערכה. (תרגיל לא לגמרי טריביאלי, מסתמך על החומר בהמשך.) ∎

הוכחה של דוגמה 1.7(3): תחילה נבדוק ש־v מקיימת את (א),(ב), (ג) של הגדרה 1.6 עבור $F[x]$ במקום F:

(א) נניח $f = \sum_k a_k x^k, g = \sum_k b_k x^k \in F[x]$, שונים מאפס. אז $fg = \sum_n c_n x^n$, באשר $c_n = \sum_{k+\ell=n} a_k b_\ell$ לכל $n \geq 0$. יהיו $i, j \geq 0$ כך ש־ $v(f) = \big(w(a_i), i\big), v(g) = \big(w(b_j), j\big)$. (נשים לב שבפרט $a_i, b_j \neq 0$.) לפי ההגדרה של v זה אומר שלכל $k, \ell \geq 0$

(i) $w(a_k) \geq w(a_i)$, וביתר דיוק $w(a_k) > w(a_i)$ או $w(a_k) = w(a_i)$ ו־$k \geq i$;

(ii) $w(b_\ell) \geq w(b_j)$, וביתר דיוק $w(b_\ell) > w(b_j)$ או $w(b_\ell) = w(b_j)$ ו־$\ell \geq j$.

מכאן $w(a_k b_\ell) \geq w(a_i b_j)$. אך אם $k < i$ אז אפילו $w(a_k) > w(a_i)$ ולכן $w(a_k b_\ell) > w(a_i b_j)$. באופן דומה, אם $\ell < j$ אז $w(a_k b_\ell) > w(a_i b_j)$.

אבל אם $k + \ell = i + j$ אז $k < i$ או $\ell < j$, לכן $w(a_k b_\ell) > w(a_i b_j)$. מכאן לפי טענה 1.10(ג)

$$w(c_{i+j}) = w\Big(\sum_{k+\ell=i+j} a_k b_\ell\Big) = w(a_i b_j).$$

ובפרט

(iii) $\big(w(c_{i+j}), i+j\big) = \big(w(a_i), i\big) + \big(w(b_j), j\big)$.

ואילו אם $n \neq i + j$ אז לפי טענה 1.10(ד)

$$w(c_n) = w\Big(\sum_{k+\ell=n} a_k b_\ell\Big) \geq \min_{k+\ell=n} w(a_k b_\ell) \geq w(a_i b_j) = w(c_{i+j}).$$

אם זה שוויון, כלומר, $w(c_n) = w(c_{i+j})$, אז יש k, ℓ כך ש־$k + \ell = n$ ו־$w(a_k b_\ell) = w(a_i b_j)$, כלומר, $w(a_k) + w(b_\ell) = w(a_i) + w(b_j)$, ומכאן, לפי (i), (ii), $w(a_k) = w(a_i)$, $w(b_\ell) = w(b_j)$. שוב, לפי (i), (ii), $k \geq i, \ell \geq j$, לכן $\big(w(c_n), n\big) \geq \big(w(c_{i+j}), i+j\big)$. לפי (iii), אגף ימין הוא $v(f) + v(g)$. לכן $v(fg) \geq v(f) + v(g)$.

(ב) נניח $f = \sum_k a_k x^k, g = \sum_k b_k x^k \in F[x]$, כך ש־$g \neq -f$. אז יש $i, \ell \geq 0$ כך ש־

$$v(f) = \big(w(a_i), i\big) = \min_k \big((w(a_k), k\big), \;\; v(f+g) = \big(w(a_\ell+b_\ell), \ell\big) = \min_k \big(w(a_k)+w(b_k), k\big).$$

מטעמי סימטריה, בלי הגבלת הכלליות, $w(a_\ell) \leq w(b_\ell)$, אחרת נחליף בין f ל־g. אז

$$w(a_\ell + b_\ell) \geq \min(w(a_\ell), w(b_\ell)) = w(a_\ell) \geq w(a_i). \qquad (*)$$

אם $w(a_\ell + b_\ell) > w(a_i)$, אז, לפי הגדרת v, מקבלים $v(f+g) > v(f) \geq \min(v(f), v(g))$.

אם $w(a_\ell + b_\ell) = w(a_i)$, אז, בגלל $(*)$ חייב להתקיים $w(a_\ell) = w(a_i)$. אבל כיוון ש־ $\big(w(a_\ell), \ell\big) \geq \big(w(a_i), i\big)$, מתקיים $\ell \geq i$. לכן $v(f+g) \geq v(f)$ גם במקרה זה.

(ג) ברור, לפי ההגדרה.

כעת נשתמש בתרגיל 1.11 כדי להרחיב את ההגדרה של v באופן יחיד על שדה המנות $F(x)$ של $F[x]$.

∎

תרגיל 1.13: *תהי v הערכה על שדה F. אז $\mathcal{O}_v := \{a \in F |\ v(a) \geq 0\}$ הוא חוג הערכה בעל שדה מנות F; הוא נקרא* **חוג ההערכה של** *v. מתקיים $\mathcal{O}_v^\times = \{a \in F |\ v(a) = 0\}$. להערכות שקולות אותו חוג הערכה.*

פתרון תרגיל 1.13: יהיו $a, b \in \mathcal{O}_v$. אז $v(a+b) \geq \min(v(a), v(b)) \geq 0$, לכן $a + b \in \mathcal{O}_v$. כמו כן $v(ab) = v(a) + v(b) \geq 0$, לכן $ab \in \mathcal{O}_v$. לבסוף, $v(\pm 1) = 0$, לכן $\pm 1 \in \mathcal{O}_v$. לכן $\mathcal{O}_v$ תת חוג של F.

יהי $a \in F^\times$. אם $v(a) \geq 0$, אז $a \in \mathcal{O}_v$. אחרת $v(a^{-1}) \geq 0$, ולכן או $a^{-1} \in \mathcal{O}_v$. לכן $\mathcal{O}_v$ חוג הערכה. ברור ש־F הוא שדה המנות שלו.

שאר הטענות הן טריביאליות. ∎

תרגיל 1.21: *הראו כי*

(א) *הערכות v, v' של שדה F שקולות אם ורק אם קיים איזומורפיזם חבורות שומר סדר $\lambda\colon v(F^\times) \to v'(F^\times)$ כך ש־ $v' = \lambda \circ v$.*

(ב) *אתרים φ, φ' של שדה F שקולים אם ורק אם קיימת העתקה חד חד ערכית ועל $\lambda\colon \varphi(F) \to \varphi'(F)$ כך ש־ $\lambda(\infty) = \infty$, $\lambda\colon \varphi(F) \smallsetminus \{\infty\} \to \varphi'(F) \smallsetminus \{\infty\}$ הוא איזומורפיזם של שדות, ו־ $\varphi' = \lambda \circ \varphi$.*

פתרון תרגיל 1.21: (א) נניח ש־v, v' שקולות. אז $v(a) = 0 \Leftrightarrow v'(a) = 0$ לכל $a \in F^\times$. לכן לאפימורפיזמים $v\colon F^\times \to v(F^\times) v'\colon F^\times \to v'(F^\times)$ יש אותו הגרעין. לפי משפט איזומורפיזם הראשון לחבורות יש איזומורפיזם $\lambda\colon v(F^\times) \to v'(F^\times)$ כך ש־$v' = \lambda \circ v$. הכיוון ההפוך ברור.

(ב) נניח שקיים λ כזה. אם $\bar{x} := \varphi(x) \neq \infty$ אז $\varphi'(x) = \lambda(\bar{x}) \neq \infty$; אם $\bar{x}' := \varphi'(x) \neq \infty$ אז $\varphi(x) = \lambda^{-1}(\bar{x}') \neq \infty$. לכן φ, φ' שקולים.

להיפך, נניח כי φ, φ' שקולים. אז לשניהם אותו חוג הערכה

$$\mathcal{O} := \{x \in F |\ \varphi(x) \neq \infty\} = \{x \in F |\ \varphi'(x) \neq \infty\}.$$

יהיו $K = \varphi(F) \smallsetminus \{\infty\}, K' = \varphi'(F) \smallsetminus \{\infty\}$. אז הצמצומים של φ, φ' ל־$\mathcal{O}$ הם אפימורפיזמים של חוגים $\varphi_0\colon \mathcal{O} \to K, \varphi_0'\colon \mathcal{O} \to K'$, ולשנים אותו הגרעין ($\mathcal{O}$ האידאל המרבי היחיד של). לפי משפט איזומורפיזם הראשון לחוגים יש איזומורפיזם $\lambda\colon K \to K'$ כך ש־$\varphi_0' = \lambda \circ \varphi_0$. נרחיב את λ להעתקה $\lambda\colon K \cup \{\infty\} \to K' \cup \{\infty\}$ על ידי $\lambda(\infty) = \infty$. אז $\varphi' = \lambda \circ \varphi$. ∎

תרגיל 6.3: *הראה ששדה הפונקציות הרציונליות מעל K הוא שדה פונקציות אלגבריות במשתנה אחד.*

פתרון תרגיל 6.3: ההרחבה $K(t)/K$ נוצרת על ידי איבר טרנסצנדטי אחד, t. לכן נותר להוכיח ש־K הוא שדה הקבועים של $K(t)$ מעל K.

יהי K' שדה הקבועים, $K \subseteq K' \subseteq K(t)$. נניח בשלילה ש־$K' \supsetneq K$. אז יש $\alpha \in K' \setminus K$. כיוון ש־$\alpha \in K(t)$, קיימים פולינומים $f(t), g(t) \in K[t]$ כך ש־$g(t) \neq 0$ ו־$\alpha = \frac{f(t)}{g(t)}$.

אז t שורש של הפולינום $f(X) - \alpha g(X) \in K'[X]$. פולינום זה אינו פולינום האפס, כי יש מקדם של αg (שהינו איבר שונה מאפס של K מוכפל ב־α) שאינו ב־K, וכל מקדמי f הם ב־K. לכן t אלגברי מעל K'. אבל K' הרחבה אלגברית של K, לכן t אלגברי מעל K. סתירה. ∎

תרגיל 12.5: *הראה שבתנאים של משפט הקירוב החזק (משפט 12.4) אפשר לדרוש $v_\mathfrak{p}(x - x_\mathfrak{p}) \geq m_\mathfrak{p}$ במקום $v_\mathfrak{p}(x - x_\mathfrak{p}) = m_\mathfrak{p}$ לכל $\mathfrak{p} \in S$.*

הוכחה: לפי משפט 12.4 יש $y \in F$ כך ש־$v_\mathfrak{p}(y - x_\mathfrak{p}) \geq m_\mathfrak{p} + 1$ לכל $\mathfrak{p} \in S$ ו־$v_\mathfrak{p}(y) \geq 0$ לכל $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$. לכל $\mathfrak{p} \in S$ נבחר $b_\mathfrak{p} \in F$ כך ש־$v_\mathfrak{p}(b_\mathfrak{p}) = m_\mathfrak{p}$. לפי משפט 12.4 יש $z \in F$ כך ש־$v_\mathfrak{p}(z - b_\mathfrak{p}) \geq m_\mathfrak{p} + 1$ לכל $\mathfrak{p} \in S$ ו־$v_\mathfrak{p}(z) \geq 0$ לכל $\mathfrak{p} \notin S \bigcup \{\mathfrak{q}\}$. נגדיר $x = y + z$. אז $x - x\mathfrak{p} = (y - x_\mathfrak{p}) + (z - b_\mathfrak{p}) + b_\mathfrak{p}$, לכן $v_\mathfrak{p}(x - x_\mathfrak{p}) = \min\left(v_\mathfrak{p}(y - x_\mathfrak{p}), v_\mathfrak{p}(z - b_\mathfrak{p}), v_\mathfrak{p}(b_\mathfrak{p})\right) = m_\mathfrak{p}$ לכל $\mathfrak{p} \in S$ ו־$v_\mathfrak{p}(x) \geq \min\left(v_\mathfrak{p}(y), v_\mathfrak{p}(z)\right) \geq 0$ לכל $\mathfrak{p} \notin S \bigcup \{\mathfrak{q}\}$. ∎

תרגיל 12.6: *הראה שאם נחליף במשפט 12.4 את התנאי $\mathfrak{p} \notin S \bigcup \{\mathfrak{q}\}$ ב־$\mathfrak{p} \notin S$, המשפט לא יהיה נכון.*

הוכחה: תהי $S = \{\mathfrak{p}_0\}$ בת איבר אחד. יהי $x_0 \in F$ כך ש־$v_{\mathfrak{p}_0}(x_0) = 1$. יהי $x \in F$ כך ש־$v_{\mathfrak{p}_0}(x - x_0) \geq 2$. אז $x \neq 0$ ו־$v_{\mathfrak{p}_0}(x) \geq 1$. לכן $(x)_0 \neq 0$ ולכן גם $(x)_\infty \neq 0$ (כי $\deg(x) = 0$). לכן יש $\mathfrak{q} \in \mathbb{P}$ כך ש־$v_\mathfrak{q}(x) < 0$. ∎

תרגיל 14.2: *הוכח שכל מחלק ממעלה 0 של $K(t)/K$ הוא ראשי. הסק שחבורת מחלקות המחלקים איזומורפית ל־$\mathbb{Z}$.*

הוכחה: יהי $\mathfrak{a} = \sum_p n_p \mathfrak{p} + n_\infty \mathfrak{p}_\infty$ מחלק של $K(t)/K$. נניח ש־$\deg \mathfrak{a} = 0$, כלומר, $\sum_p n_p \deg p + n_\infty = 0$, ומכאן $n_\infty = -\sum_p n_p \deg p$. יהי

$$f = \prod_p p^{n_p} \in K(t).$$

אז

(א) $v_p((f)) = n_p = v_p(\mathfrak{a})$;

(ב) $v_\infty(f) = -\deg f = -\sum_p n_p \deg p = n_\infty = v_\infty(\mathfrak{a})$.

לכן $(f) = \mathfrak{a}$. ∎

תרגיל 14.3: *יהי* $\mathfrak{a}$ *מחלק של* $K(t)/K$*. אז* $\dim \mathfrak{a} = \max(0, \deg \mathfrak{a} + 1)$.

הוכחה: נזכור ש־$g = 0$.

אם $\deg \mathfrak{a} < 0$, זאת מסקנה 12.2(ג); אם $\deg \mathfrak{a} \geq 0$, זאת מסקנה 12.2(ה). ∎

תרגיל 14.4: *יהי* $0 \neq f \in K[t]$ *פולינום. אז* $\deg(f)_0 = \deg f$.

הוכחה: בדיון בפרק 14 הראינו, לכל $0 \neq f \in K(t)$,

$$(f) = \sum_p n_p p - (\deg f)\mathfrak{p}_\infty. \tag{2}$$

אם f פולינום, אז $(f)_0 = \sum_p n_p p,\ (f)_\infty = (\deg f)\mathfrak{p}_\infty$. בפרט

$\deg(f)_0 = \deg(f)_\infty = \deg f \cdot \deg \mathfrak{p}_\infty = \deg f$. ∎

תרגיל 16.4: *יהי* F/K *שדה פונקציות אלגבריות בעל גזע* 0*. הוכח שכל מחלק שלו ממעלה* 0 *הוא ראשי.*

פתרון: נניח $\deg \mathfrak{a} = 0$. כיוון ש־ $\deg \mathfrak{a} > 2g - 2 = -2$, מתקיים $\dim \mathfrak{a} = \deg \mathfrak{a} + 1 - g = 1$. לפי מסקנה 12.2(ד), $\mathfrak{a}$ ראשי. ∎

תרגיל 20.12: *נניח כי* F/E *נורמלית. הוכח*

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Aut}(F/E) |\ v_{\mathfrak{P}}(\sigma z - z) \geq 0 \text{ לכל } z \in \mathcal{O}_{\mathfrak{P}}\},$$

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Aut}(F/E) |\ v_{\mathfrak{P}}(\sigma z - z) > 0 \text{ לכל } z \in \mathcal{O}_{\mathfrak{P}}\}.$$

הוכחה: (א) אם $\sigma \in D(\mathfrak{P})/\mathfrak{p})$ אז $\sigma\mathfrak{P} = \mathfrak{P}$ ולכן $\sigma^{-1}\mathfrak{P} = \mathfrak{P}$. יהי $z \in \mathcal{O}_{\mathfrak{P}}$, אז $v_{\mathfrak{P}}(z) \geq 0$ ו־$v_{\mathfrak{P}}(\sigma z) = v_{\sigma^{-1}\mathfrak{P}}(z) = v_{\mathfrak{P}}(z) \geq 0$, ומשני האי שוויונים נובע $v_{\mathfrak{P}}(\sigma z - z) \geq 0$.

להיפך, נניח $v_{\mathfrak{P}}(\sigma z - z) \geq 0$ לכל $z \in \mathcal{O}_{\mathfrak{P}}$. כל z כזה מקיים גם $v_{\mathfrak{P}}(z) \geq 0$, ולכן $v_{\mathfrak{P}}(\sigma z) \geq 0$, כלומר, $\sigma z \in \mathcal{O}_{\mathfrak{P}}$. לכן $\sigma\mathcal{O}_{\mathfrak{P}} \subseteq \mathcal{O}_{\mathfrak{P}}$.

נראה הכלה הפוכה. יהי $z \in \mathcal{O}_{\mathfrak{P}}$. בגלל ש־$z$ אלגברי מעל E, יש $n > 1$ כך ש־$\sigma^n z = z$. לפי הפסקה הקודמת $x := \sigma^{n-1} z \in \mathcal{O}_{\mathfrak{P}}$, ו־$z = \sigma x \in \sigma\mathcal{O}_{\mathfrak{P}}$. לכן $\sigma\mathcal{O}_{\mathfrak{P}} \supseteq \mathcal{O}_{\mathfrak{P}}$.

השוויון $\sigma\mathcal{O}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}$ שקול ל־$\sigma\mathfrak{P} = \mathfrak{P}$, כלומר, $\sigma \in D(\mathfrak{P})$.

(ב) אם $\sigma \in I(\mathfrak{P}))$ אז $\sigma \in D(\mathfrak{P}))$ ולכל $z \in \mathcal{O}_{\mathfrak{P}}$ מתקיים $\bar{z} = \overline{\sigma z}$. מכאן $\overline{\sigma z - z} = 0$, כלומר, $v_{\mathfrak{P}}(\sigma z - z) > 0$.

להיפך, אם תנאי זה מתקיים לכל $z \in \mathcal{O}_{\mathfrak{P}}$, אז, לפי (א), $\sigma \in D(\mathfrak{P})$ ולכל $z \in \mathcal{O}_{\mathfrak{P}}$ מתקיים $\overline{\sigma z} = \bar{z}$. מכאן $\bar{\sigma} = 1$, לכן $\sigma \in I(\mathfrak{P})$. ∎

תרגיל 21.4: *אם* L/K *הרחבה פשוטה (בפרט, אם* L/K *פרידה סופית) אז* $[F : E]/[L : K] \in \mathbb{N}$.

הוכחה: נניח $L = K(\alpha)$. אז $LE = E(\alpha)$. יהי f הפולינום האי פריק של α מעל K. לפי בתרגיל 6.7, f הוא הפולינום האי פריק של α מעל E. בפרט $[L : K] = \deg f = [LE : E]$. לכן $[F : E]/[L : K] = [F : E]/[LE : E] = [F : LE] \in \mathbb{N}$. ∎

תרגיל 22.8: *יהי E/K שדה פונקציות. נניח ש־K משוכלל (כל הרחבה סופית שלו פרידה). הראה שיש L/K סופית כך שלהרחבת שדה המקדמים LE/L יש מחלק ראשוני בעל מעלה 1.*

הוכחה: יהיו $\mathfrak{p}$ מחלק ראשוני של E. ניקח $L = E_{\mathfrak{p}}$. אם $\mathfrak{P}$ מונח מעל $\mathfrak{p}$, אז לפי משפט 22.6, $F_{\mathfrak{P}} = E_{\mathfrak{p}}L = L$. לכן $\deg \mathfrak{P} = [F_{\mathfrak{P}} : L] = 1$. ∎

תרגיל 32.8: *יהי $\mathcal{O}$ **חוג הערכה בדידה**, כלומר, חוג הערכה שחבורת ההערכה שמתאימה לו איזומורפית ל־$\mathbb{Z}$. אז $\mathcal{O}$ חוג ראשי. יתר על כן, (לא רק שכל אידאל של $\mathcal{O}$ ראשי, אלא גם) כל מודול־$\mathcal{O}$ שמוכל ממש בשדה המנות של $\mathcal{O}$ הוא מהצורה $M = t\mathcal{O}$, באשר t בעל ההערכה המזערית ב־M.*

הוכחה: תהי v ההערכה המתאימה ל־$\mathcal{O}$ ויהי F שדה המנות של $\mathcal{O}$. יהי $M \subsetneqq F$ מודול־$\mathcal{O}$.

אם $M = 0$, אז $M = 0 \cdot \mathcal{O}$, מה שמוכיח את הטענה. נניח, אם כן, כי $M \neq 0$.

אם $0 \neq t \in M$ ו־$t' \in F$ כך ש־$v(t') \geq v(t)$, אז $v(\frac{t'}{t}) \geq 0$, לכן $\frac{t'}{t} \in \mathcal{O}$, ולכן $t' = \frac{t'}{t}t \in M$ וגם $t' = \frac{t'}{t}t \in t\mathcal{O}$. כיוון שלא כל $t' \in F$ הוא ב־M, מכאן ברור שיש $0 \neq t \in M$ בעל הערכה מזערית ומתקיים

$$M = \{t' \in F |\ v(t') \geq v(t)\} = t\mathcal{O}.$$

בפרט, אם M הוא אידאל־$\mathcal{O}$, אז הוא ראשי. (למעשה, הוכחנו את זה רק אם $M \neq F$; אבל אם $M = F$, אז, כיוון ש־$M \subseteq \mathcal{O}$, גם $F = \mathcal{O}$, וזה חוג ראשי.) ∎