14 ספרביליות

14.1 פולינומים ספרביליים והרחבות ספרביליות

יהיו K שדה, $f \in K[x]$ פולינום ממעלה n ו-L/K הרחבת שדות שבה f מתפצל. כלומר,

$$f = c(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n) \in L[x].$$

שורש פשוט

- נאמר כי $\alpha = \alpha_i \in L$ הוא **שורש פשוט** (simple root) של f אם הוא מופיע בדיוק פעם אחת בפיצול, כלומר, אם $(x-\alpha) \mid f$ אבל $(x-\alpha)^2 \nmid f$.

שורש מרובה

- נאמר כי α **שורש מרובה** (multiple root) של f אם הוא מופיע בפיצול לפחות פעמיים, כלומר, אם $(x-\alpha)^2 \mid f$.

כזכור, לכל פולינום מעל K יש שדה הרחבה L שבו הוא מתפצל. למשל, ניתן לקחת את הסגור האלגברי של K (משפט 11.46). הרחבה מינימלית של K שבה f מתפצל נקראת, כאמור, שדה פיצול.

פולינום ספרבילי

הגדרה 14.1 הפולינום $f \in K[x]$ נקרא **ספרבילי (פריד)** אם אין לו שורשים מרובים בשדה הרחבה L שבו הוא מתפצל.

לכאורה, תכונת הספרביליות של f תלויה בשדה ההרחבה L שבחרנו. מיד נראה (מסקנה 14.7) כי, למעשה, היא אינה תלויה ב-L. מושג **הנגזרת** יועיל לנו בהשגת תובנה זו.

הנגזרת

f'

הגדרה 14.2 בהינתן $f = \sum_{i\geq 0} a_i x^i \in K[x]$ נגדיר באופן פורמלי את **הנגזרת**[1] של f בתור:

$$f' = \sum_{i\geq 1} i a_i x^{i-1} \in K[x],$$

כאשר $i = \underbrace{1+\ldots+1}_{\text{פעמים } i} \in K$.

אם $\mathrm{char}K = 0$ אז $\deg(f') = \deg(f) - 1$. לעומת זאת, אם $\mathrm{char}K = p$ (p ראשוני), הנגזרת עשויה להיות ממעלה קטנה יותר מ-$(\deg(f)-1)$. למשל,

$$(x^p - a)' = px^{p-1} = 0.$$

תרגיל 14.3 הוכיחו כי כללי הנגזרת המוכרים מאנליזה מתקיימים גם בעבור הנגזרת הפורמלית: הראו שלכל $f, g \in K[x]$ ולכל $n \in \mathbb{N}$ מתקיים

1. $(f+g)' = f' + g'$
2. $(fg)' = f'g + fg'$
3. $(f^n)' = nf^{n-1}f'$

[1] שימו לב שהנגזרת כאן היא מושג פורמלי שקשור רק חלקית למושג הנגזרת המוכר לכם מתחום החשבון הדיפרנציאלי והאינטגרלי (חדו״א). כאן איננו חושבים על הפולינומים כעל פונקציות אלא כעל ישויות אלגבריות פורמליות. למשל, לנגזרת מתחום החדו״א אין משמעות כאשר מדובר בפולינום מעל שדה סופי, אך הנגזרת כאן מוגדרת היטב גם במקרה זה.

טענה 14.4 יהיו L/K הרחבת שדות, $f\in K[x]$ פולינום שמתפצל ב-L ו-$\alpha\in L$ שורש של f. אזי α שורש מרובה של f אם ורק אם $f'(\alpha)=0$, כלומר, אם ורק אם $(x-\alpha)\,|f'$.

הוכחה: בחוג $L[x]$ ניתן לכתוב

$$f(x)=c\prod_{j=1}^{r}(x-\alpha_j)^{e_j}$$

כאשר עכשיו ה-α_j-ים שונים זה מזה. לפי תרגיל 14.3,

$$f'(x)=c\sum_{j=1}^{r}\left(e_j(x-\alpha_j)^{e_j-1}\prod_{k\neq j}(x-\alpha_k)^{e_k}\right).$$

בלי הגבלת הכלליות $\alpha=\alpha_1$ ואז

$$f'(\alpha)=c\sum_{j=1}^{r}\left(e_j(\alpha_1-\alpha_j)^{e_j-1}\prod_{k\neq j}(\alpha_1-\alpha_k)^{e_k}\right)=ce_1(\alpha_1-\alpha_1)^{e_1-1}\prod_{k\neq 1}(\alpha_1-\alpha_k)^{e_k}.$$

אם α שורש מרובה, כלומר אם $e_1\geq 2$, ביטוי זה מתאפס. אם α שורש פשוט, כלומר, אם $e_1=1$, אז $e_1\neq 0$ בשדה K וכל יתר הגורמים אף הם אינם מתאפסים ועל כן הביטוי כולו אינו מתאפס. ■

נזכיר כי לכל שני פולינומים $f,g\in K[x]$ סימנו ב-(f,g) את ה-gcd שלהם (הגדרה 10.64). ניתן לחשב את (f,g) לפי האלגוריתם של אוקלידס, שנשען, מצדו, על סדרה של חלוקות עם שארית (ראו סעיף 10.6). למשל, בשלב הראשון של האלגוריתם, אם $\deg f\geq\deg g$, אנו מוצאים $q,r\in K[x]$ כך ש-$f=qg+r$ ו-$\deg r<\deg g$, ואז, תוך שימוש בעובדה ש-$(f,g)=(g,r)$, ממשיכים באלגוריתם עם הזוג g,r במקום f,g. כדי למצוא את q ואת r, נזקקנו רק לפעולות השדה (חיבור, חיסור, כפל וחילוק) במקדמים של f ו-g. בפרט, האלגוריתם של אוקלידס היה נותן בדיוק אותה תוצאה גם לו חשבנו על הפולינומים f ו-g כעל פולינומים ב-$L[x]$, בעבור L, שדה הרחבה כלשהו של K. קיבלנו:

טענה 14.5 אם $f,g\in K[X]$ ו-L/K הרחבה כלשהי, אז בין אם נחשוב על f ועל g כעל פולינומים ב-$K[x]$ ובין אם נחשוב עליהם כעל פולינומים ב-$L[x]$, (f,g) יהיה אותו פולינום (ב-$K[x]$).

משפט 14.6 פולינום $f\in K[x]$ הוא ספרבילי אם ורק אם $(f,f')=1$.

לפני שנוכיח את המשפט, נעיר שלכאורה, היינו צריכים לציין בתנאי המשפט גם את שדה ההרחבה L שבו f מתפצל. אולם, מכיוון שהתנאי $(f,f')=1$ אינו תלוי, כאמור, בשדה ההרחבה, נסיק:

מסקנה 14.7 תכונת הספרביליות של פולינום **אינה** תלויה בשדה ההרחבה L שבו הוא מתפצל.

הוכחת משפט 14.6: יהי L שדה הרחבה של K שבו f מתפצל. לפי טענה 14.5, ניתן לחשב את (f,f') בתוך $L[x]$. אבל מעל L, f מתפצל למכפלה של גורמים לינאריים:

$$f(x)=c\prod_{j=1}^{r}(x-\alpha_j)^{e_j}.$$

אם יש ל-f שורש מרובה α_j, אזי $(x-\alpha_j)\mid f$ וגם $(x-\alpha_j)\mid f'$ (לפי טענה 14.4), ולכן $(x-\alpha_j)\mid(f,f')$ ובפרט $(f,f')\neq 1$. מצד שני, אם f ספרבילי, כלומר נטול שורשים מרובים, אז $(x-\alpha_j)\nmid f'$ לכל j, כלומר f' אינו מתחלק באף גורם אי-פריק של f ולפיכך $(f,f')=1$. ■

תרגיל 14.8 בסימונים דלעיל, הוכיחו כי כאשר $\mathrm{char}K = 0$ מתקיים

$$(f, f') = \prod_{j=1}^{r} (x - \alpha_j)^{e_j - 1} \; .$$

מה משתבש כאשר $\mathrm{char}K = p$?

כפי שנראה בהמשך, תכונת הספרביליות מעניינת במיוחד כאשר מדובר בפולינומים אי-פריקים. נבחין בין שדות ממציין 0 לבין שדות ממציין p.

מסקנה 14.9 אם $\mathrm{char}K = 0$ אז כל פולינום **אי-פריק** מעל K הוא ספרבילי.

הוכחה: המחלק המשותף המקסימלי (f, f') הוא מחלק הן של f והן של f' ב-$K[x]$. אם $\deg f = n$ אז $\deg f' = n - 1$, ולכן (f, f') חייב להיות מחלק ממש של f (כלומר, מחלק ששונה מ-f עצמו ומחבריו בחוג $K[x]$). מכיוון ש-f אי-פריק, מחלק זה הוא בהכרח 1 (עד כדי חברות). $\blacksquare$

דוגמה 14.10 יהי $K = \mathbb{F}_p(t)$, ויהי $f = x^p - t \in K[x]$. ראינו כי פולינום זה הוא אי-פריק (תרגיל 10.106). אבל, אם α שורש של f בשדה הרחבה של K, אז

$$f = x^p - \alpha^p = (x - \alpha)^p \; ,$$

ולכן f אינו ספרבילי. כמובן, גם תנאי הנגזרת עובד כאן (בדקו זאת!). נסיק כי לא ניתן לוותר על התנאי $\mathrm{char}K = 0$ במסקנה 14.9.

את הדוגמה האחרונה נכליל בטענה הבאה שעוסקת בפולינומים אי-פריקים מעל שדה ממציין ראשוני. אם K שדה ממציין ראשוני p ו-$f = \sum a_i x^i \in K[x]$, נסתכל בקבוצת המעריכים של המונומים שאינם אפס שמרכיבים את f, כלומר ב-$\{i \mid a_i \neq 0\}$, ותהי p^e החזקה הגבוהה ביותר של p שמחלקת את כולם. למשל, אם $f = 4x^{2p^3} - x^{p^3} + x^{4p^2} + 2$ (ו-$p \neq 2$), ניקח $e = 2$.

טענה 14.11 יהיו K שדה ממציין ראשוני p, $f \in K[x]$ פולינום **אי-פריק** ו-p^e כנ"ל. אזי

1. $f(x) = h\left(x^{p^e}\right)$ כאשר $h \in K[x]$ פולינום אי-פריק **וספרבילי**.
2. הריבוי של כל שורש של f הוא בדיוק p^e.

למשל, בדוגמה 14.10, $e = 1$ ו-$h = x - t$ הוא אכן פולינום אי-פריק וספרבילי שמקיים $f(x) = h(x^p)$. הריבוי של השורש היחידי של f הוא אכן p.

הוכחה: (1) ראשית, נשים לב כי f עצמו ספרבילי אם ורק אם $e = 0$: הרי כמו בהוכחה של מסקנה 14.9, אם $e = 0$, $f' \neq 0$ וכן $\deg f' < \deg f$, לכן $(f, f') = 1$ (נזכיר כי לפי ההנחה f אי-פריק). מאידך, אם $e \neq 0$ אז $f' = 0$ ואז $(f, f') = f \neq 1$ ולכן f אינו ספרבילי. לפיכך, אם $e = 0$ סיימנו.

אם $e \geq 1$, אזי

$$f = b_r x^{rp^e} + b_{r-1} x^{(r-1)p^e} + \ldots + b_1 x^{p^e} + b_0 \; ,$$

כך ש-$b_r \neq 0$ וכן קיים $1 \leq i \leq r$ עם $p \nmid i$ ו-$b_i \neq 0$ (אחרת e לא היה החזקה המקסימלית של p שמחלקת את כל המעריכים). נגדיר $h(x) = b_r x^r + b_{r-1} x^{r-1} + \ldots + b_0$ ואז ברור כי $f(x) = h\left(x^{p^e}\right)$ וכי h ספרבילי (כי בעבורו $e = 0$). נותר להראות כי h אי-פריק. זה נובע מכך שכל פירוק $h(x) = q(x) r(x)$ נותן אוטומטית גם פירוק $f(x) = q\left(x^{p^e}\right) r\left(x^{p^e}\right)$, בסתירה לכך ש-$f$ אי-פריק.

(2) יהי L שדה הרחבה של K שבו f ו-h מתפצלים, ויהיו $\beta_1,\ldots,\beta_r\in L$ השורשים השונים של h (זכרו כי h ספרבילי), כלומר $h\left(x\right)=c\left(x-\beta_1\right)\ldots\left(x-\beta_r\right)$. אך אז מתקיים:

$$.f\left(x\right)=h\left(x^{p^e}\right)=c\left(x^{p^e}-\beta_1\right)\ldots\left(x^{p^e}-\beta_r\right)$$

לכן, כל שורש $\alpha\in L$ של f הוא שורש של אחד הגורמים $\left(x^{p^e}-\beta_i\right)$, ומתקיים אז $\alpha^{p^e}=\beta_i$, ולכן

$$.\left(x^{p^e}-\beta_i\right)=\left(x^{p^e}-\alpha^{p^e}\right)=\left(x-\alpha\right)^{p^e}$$

(כדי להשתכנע בשוויון האחרון ניתן, למשל, להפעיל את למה 13.6 כמה פעמים ולקבל שבשדה ממציין p מתקיים

$$(.\left(a+b\right)^{p^e}=\left(\left(a+b\right)^p\right)^{p^{e-1}}=\left(a^p+b^p\right)^{p^{e-1}}=\left(a^{p^2}+b^{p^2}\right)^{p^{e-2}}=\ldots=a^{p^e}+b^{p^e}$$

מכיוון שבברור α אינו מאפס את $\left(x^{p^e}-\beta_j\right)$ אם $j\neq i$, הריבוי של α כשורש של f הוא בדיוק p^e. ■

ממסקנה 14.9 ומטענה 14.11 נסיק:

מסקנה 14.12 יהי K שדה כלשהו ו-$f\in K\left[x\right]$ אי-פריק, אזי לכל השורשים של f אותו ריבוי, וריבוי זה אינו תלוי בשדה ההרחבה שבו f מתפצל.

הרחבה ספרבילית

הגדרה 14.13 תהי L/K הרחבה אלגברית של שדות.
איבר $\alpha\in L$ ייקרא **ספרבילי** (**פריד**) מעל K אם הפולינום המינימלי שלו מעל K הוא ספרבילי. איבר ספרבילי
ההרחבה L/K תקרא **ספרבילית** (**פרידה**) אם כל איבריה ספרביליים. הרחבה ספרבילית

שימו לב שלפי ההגדרה, המונח "הרחבה ספרבילית" מתייחס רק להרחבות אלגבריות.

טענה 14.14 בשדות ממציין 0, כל הרחבה אלגברית היא ספרבילית.

הוכחה: הפולינום המינימלי של איבר הוא אי-פריק, וראינו (מסקנה 14.9) כי כל פולינום אי-פריק מעל שדה ממציין 0 הוא ספרבילי. ■

תרגיל 14.15 אם L/K הרחבה ספרבילית ו-$K\subseteq M\subseteq L$ שדה ביניים, אז גם L/M וגם M/K ספרביליות.

תרגיל 14.16 אם $\mathrm{char}K=p$ ו-$[L:K]$ זר ל-p, אז L/K ספרבילית.

תרגיל 14.17 יהי K שדה ויהי n טבעי.
1. אם $\mathrm{char}K=p$ הניחו בנוסף כי $(n,p)=1$. הוכיחו כי קיים שורש יחידה פרימיטיבי מסדר n בסגור האלגברי של K (ראו הגדרה 13.22).
2. מצאו דוגמה לשדה K ולמספר n כך **שאין** שורש יחידה פרימיטיבי מסדר n בסגור האלגברי של K.

14.2 הרחבת שיכונים של שדות

תהי ${}^{L}\!/\!{}_{K}$ הרחבה סופית של שדות, ונניח כי $\varphi : K \hookrightarrow \Omega$ הוא שיכון של K לתוך שדה **סגור אלגברית**[2] Ω. (למשל, ניתן לקחת את השיכון של K בתוך הסגור האלגברי שלו — ראו משפט 11.46). בסעיף זה נתמקד בשאלה: כמה הרחבות של φ יש לשיכונים של L כולו? נסמן את מספר ההרחבות ב-$i_\varphi\left({}^{L}\!/\!{}_{K}\right)$, כלומר $\boxed{i_\varphi\left({}^{L}\!/\!{}_{K}\right)}$

$$.i_\varphi\left({}^{L}\!/\!{}_{K}\right) = \#\left\{\widehat{\varphi} : L \hookrightarrow \Omega \;\;\middle|\;\; \widehat{\varphi}|_K = \varphi\right\}$$

מיד (משפט 14.19) נראה שתמיד יש לפחות הרחבה אחת וכי מספר השיכונים המרחיבים אינו תלוי לא בשדה Ω ולא בשיכון המסוים φ. לפני כן נציין שכאשר יש שיכון של שדות, למשל $\varphi : K \hookrightarrow \Omega$, ניתן להרחיבו באופן טבעי לשיכון של חוגי הפולינומים $\varphi : K[x] \hookrightarrow \Omega[x]$, לפי ההגדרה $\varphi\left(\sum c_i x^i\right) \overset{\text{def}}{=} \sum \varphi(c_i)\, x^i$. קל לראות כי זהו אכן שיכון של חוגים. יתרה מזאת, שיכון מורחב זה משרה איזומורפיזם בין חוג הפולינומים $K[x]$ לבין חוג הפולינומים $\varphi(K)[x]$.

את הניתוח של $i_\varphi\left({}^{L}\!/\!{}_{K}\right)$ נתחיל במקרה של הרחבות פשוטות.

למה 14.18 אם $L = K(\alpha)$ הרחבה פשוטה סופית, אז $i_\varphi\left({}^{L}\!/\!{}_{K}\right)$ שווה למספר השורשים **השונים** של הפולינום המינימלי של α, $m_\alpha \in K[x]$.
בפרט, תמיד קיימת לפחות הרחבה אחת של φ, ומספר ההרחבות, $i_\varphi\left({}^{L}\!/\!{}_{K}\right)$, אינו תלוי לא ב-$\Omega$ ולא ב-φ.

נזכיר כי מספר השורשים השונים של m_α מוגדר היטב (ואינו תלוי, למשל, בשדה ההרחבה שבו m_α מתפצל) לפי מסקנה 14.12.

הוכחת למה 14.18: נניח כי $m_\alpha(x) = \sum c_i x^i$. אזי בתוך L מתקיים $\sum c_i \alpha^i = 0$. אם $\widehat{\varphi} : L \to \Omega$ מרחיב את φ, מתקיים

$$0 = \widehat{\varphi}(0) = \widehat{\varphi}\left(\sum c_i \alpha^i\right) = \sum \varphi(c_i)\, \widehat{\varphi}(\alpha)^i$$

ולכן $\widehat{\varphi}(\alpha)$ הוא שורש של הפולינום $\widetilde{m}_\alpha(x) = \varphi(m_\alpha(x))$.

מצד שני, בדומה ללמה 13.14, כל הרחבה של φ ל-L כולו נקבעת לפי התמונה של α. יתר על כן, לכל שורש $\widetilde{\alpha} \in \Omega$ של $\widetilde{m}_\alpha(x)$ קיים הומומורפיזם יחיד $\widehat{\varphi} : L \to \Omega$ שמרחיב את φ והשולח את α ל-$\widetilde{\alpha}$. הומומורפיזם זה נתון דרך הרכבת האיזומורפיזמים הבאים (כאן $\widetilde{K}$ מסמן את $\varphi(K)$, תמונת K):

$$L = K(\alpha) \cong K[x] / (m_\alpha(x)) \cong \widetilde{K}[x] / (\widetilde{m}_\alpha(x)) \cong \widetilde{K}(\widetilde{\alpha})$$

(את האיזומורפיזמים הראשון והשלישי הגדרנו בטענה 11.20; האיזומורפיזם השני מתקבל מהאיזומורפיזם שמשרה φ בין $K[x]$ לבין $\widetilde{K}[x]$.) לפיכך $i_\varphi\left({}^{L}\!/\!{}_{K}\right)$ שווה למספר השורשים השונים של $\widetilde{m}_\alpha(x)$. נותר לשים לב כי מספר השורשים השונים של $\widetilde{m}_\alpha(x)$ שווה לזה של $m_\alpha(x)$, שכן φ משרה איזומורפיזם בין $K[x]$ לבין $\widetilde{K}[x]$. ■

משפט 14.19 יהי $\varphi : K \hookrightarrow \Omega$ שיכון לתוך שדה סגור אלגברית Ω. לכל הרחבה סופית ${}^{L}\!/\!{}_{K}$ מתקיים:

1. $i_\varphi\left({}^{L}\!/\!{}_{K}\right) \geq 1$ ומספר זה אינו תלוי לא ב-Ω ולא ב-φ. נסמן לכן מספר זה ב-$i\left({}^{L}\!/\!{}_{K}\right)$. $\boxed{i\left({}^{L}\!/\!{}_{K}\right)}$

[2] את המשפטים על אודות הרחבות של שיכונים שנלמד בפרק הנוכחי ובפרק הבא ניתן להוכיח גם ללא הסתמכות על קיומו של סגור אלגברי. כדי להוכיח את קיומו של סגור אלגברי לכל שדה (משפט 11.46) הזדקקנו למשפט 10.29, שבתורו הסתמך על הלמה של צורן ששקולה לאקסיומת הבחירה (ראו נספח B). ככלל, אם הדבר אפשרי, מתמטיקאים נוטים להעדיף שלא להסתמך על אקסיומת הבחירה. אנחנו החלטנו לחרוג מנטייה זו בשני פרקים אלה משום שלמיטב שיפוטנו, התורה הופכת

2. $i\left({}^{L}\!/_{K}\right)$ הוא כפלי, כלומר, אם $K \subseteq M \subseteq L$, אזי

$$.i\left({}^{L}\!/_{K}\right) = i\left({}^{L}\!/_{M}\right) \cdot i\left({}^{M}\!/_{K}\right)$$

הוכחה: נוכיח את שני הסעיפים יחד, באינדוקציה על דרגת ההרחבה $[L:K]$. אם $[L:K]=1$, כלומר $L=K$, שני הסעיפים טריוויאליים.

כעת תהי ${}^{L}\!/_{K}$ הרחבה לא טריוויאלית כלשהי. אם **לא** קיים שדה ביניים ממש $L \supsetneq M \supsetneq K$, אזי ההרחבה פשוטה (מדוע?), סעיף (1) נכון לפי הלמה (14.18), וסעיף (2) מתקיים באופן טריוויאלי.

כעת נניח כי קיים שדה ביניים ממש, ויהי M שדה כלשהו כזה (כלומר $L \supsetneq M \supsetneq K$). במקרה זה, הנחת האינדוקציה חלה על ההרחבות ${}^{L}\!/_{M}$ ו-${}^{M}\!/_{K}$. יש בדיוק $i_{\varphi}\left({}^{M}\!/_{K}\right) = i\left({}^{M}\!/_{K}\right)$ הרחבות של $\varphi\colon K \to \Omega$ לשיכונים $\widetilde{\varphi}\colon M \to \Omega$, ולפי סעיף (1) בעבור ${}^{L}\!/_{M}$, לכל שיכון כזה יש בדיוק $i_{\widetilde{\varphi}}\left({}^{L}\!/_{M}\right) = i\left({}^{L}\!/_{M}\right)$ הרחבות לשיכון $\widehat{\varphi}: L \to \Omega$.

$$\begin{tikzcd}
L \arrow[r, hook, "\widehat{\varphi}"] \arrow[d, dash] & \Omega \\
M \arrow[r, hook, "\widetilde{\varphi}"] \arrow[d, dash] & \Omega \\
K \arrow[r, hook, "\varphi"] & \Omega
\end{tikzcd}$$

מצד שני, כל שיכון של L ב-Ω שמרחיב את φ מתקבל כך (הרי יש לכל שיכון כזה צמצום לשיכון של M). לכן יש בדיוק $i\left({}^{L}\!/_{M}\right) \cdot i\left({}^{M}\!/_{K}\right)$ הרחבות של φ לשיכונים של L. כלומר, $i_{\varphi}\left({}^{L}\!/_{k}\right) = i\left({}^{L}\!/_{M}\right) \cdot i\left({}^{M}\!/_{K}\right)$ ועל כן $i_{\varphi}\left({}^{L}\!/_{K}\right)$ חיובי, אינו תלוי ב-Ω ולא ב-φ, ומקיים גם את הכפליות מסעיף (2). ■

דרגת הספרביליות של הרחבה

הגודל $i\left({}^{L}\!/_{K}\right)$ נקרא **דרגת הספרביליות** של ${}^{L}\!/_{K}$.

המשפט הבא מספק קריטריון לאבחון ספרביליות בהרחבות סופיות.

משפט 14.20 תהי ${}^{L}\!/_{K}$ הרחבת שדות סופית. אזי

$$,1 \le i\left({}^{L}\!/_{K}\right) \le [L:K]$$

והערך העליון מתקבל אם ורק אם ${}^{L}\!/_{K}$ ספרבילית, כלומר ${}^{L}\!/_{K}$ ספרבילית אם ורק אם דרגת הספרביליות שווה לדרגת ההרחבה.

הוכחה: את החסם מלמטה $1 \le i\left({}^{L}\!/_{K}\right)$ כבר ראינו (משפט 14.19). נראה את החסם מלמעלה. כל הרחבה סופית היא הרחבה נוצרת סופית: $L = K\left(\alpha_1, \ldots, \alpha_r\right)$, ולכן מתקבלת כמגדל של הרחבות פשוטות:

$$.K \subseteq K\left(\alpha_1\right) \subseteq K\left(\alpha_1\right)\left(\alpha_2\right) \subseteq \ldots \subseteq K\left(\alpha_1, \ldots, \alpha_{r-1}\right)\left(\alpha_r\right) = L$$

לפי למה 14.18 בעבור הרחבות פשוטות, $i\left({}^{K(\alpha)}\!/_{K}\right)$ שווה למספר השורשים השונים של הפולינום המינימלי של α, ובפרט

$$.i\left({}^{K(\alpha)}\!/_{K}\right) \le \deg m_{\alpha} = [K(\alpha):K]$$

נהירה יותר אם מסתמכים על קיומו של סגור אלגברי.

על-ידי הפעלה חוזרת של אותו טיעון נקבל

$$\begin{aligned} i\left({}^{L}\!/_{K}\right) &= i\left({}^{K(\alpha_1)}\!/_{K}\right)\cdot i\left({}^{K(\alpha_1,\alpha_2)}\!/_{K(\alpha_1)}\right)\cdot\ldots\cdot i\left({}^{L}\!/_{K(\alpha_1,\ldots,\alpha_{r-1})}\right)\leq \\ &\leq \left[K\left(\alpha_1\right):K\right]\cdot\left[K\left(\alpha_1,\alpha_2\right):K\left(\alpha_1\right)\right]\cdot\ldots\cdot\left[L:K\left(\alpha_1,\ldots,\alpha_{r-1}\right)\right]=\left[L:K\right] \end{aligned} \tag{15}$$

(השתמשנו r פעמים בלמה 14.18 על הרחבות פשוטות). בכך הוכחנו את החסם העליון.

כעת נוכיח את התנאי לשוויון לחסם עליון זה. ראשית, אם ${}^{L}\!/_{K}$ ספרבילית, גם כל הרחבות הביניים ${}^{K(\alpha_1,\ldots,\alpha_{i+1})}\!/_{K(\alpha_1,\ldots,\alpha_i)}$ ספרביליות (תרגיל 14.15), ולפי למה 14.18, כל האי-שוויונות ב-(15) הם למעשה שוויונות ולפיכך $i\left({}^{L}\!/_{K}\right)=\left[L:K\right]$.

מצד שני, נניח כי ההרחבה ${}^{L}\!/_{K}$ אינה ספרבילית. אזי קיים $\beta\in L$ שאינו ספרבילי מעל K. נשלים את β לקבוצת יוצרים של L: $L=K\left(\beta_1=\beta,\beta_2,\ldots,\beta_m\right)$. אם נכתוב שוב את האי-שוויון (15) בעבור קבוצת יוצרים זו, נקבל אי-שוויון ממש, שכן $\left[K\left(\beta_1\right):K\right]>i\left({}^{K(\beta_1)}\!/_{K}\right)$. ∎

מסקנה 14.21 יהיו ${}^{M}\!/_{K}$ ו-${}^{L}\!/_{M}$ הרחבות סופיות של שדות. אם שתיהן ספרביליות, אזי גם ${}^{L}\!/_{K}$ ספרבילית.

הוכחה: לפי משפטים 14.19 ו-14.20, מתקיים

$$i\left({}^{L}\!/_{K}\right)=i\left({}^{L}\!/_{M}\right)\cdot i\left({}^{M}\!/_{K}\right)=\left[L:M\right]\cdot\left[M:K\right]=\left[L:K\right]$$

ולכן ${}^{L}\!/_{K}$ ספרבילית. ∎

תרגיל 14.22 הוכיחו כי שלושת התנאים הבאים שקולים בעבור הרחבה סופית ${}^{L}\!/_{K}$:

1. ההרחבה ספרבילית.
2. **יש** קבוצת יוצרים של L מעל K שכל איבריה ספרביליים.
3. **כל** קבוצת יוצרים של L מעל K מורכבת מאיברים ספרביליים.

כמסקנה מיידית מתרגיל זה נקבל:

משפטון 14.23 שדה פיצול של פולינום ספרבילי הוא הרחבה ספרבילית.

הוכחה: אם $f\in K[x]$ ספרבילי ו-L שדה פיצול שלו מעל K, אזי $L=K\left(\alpha_1,\ldots,\alpha_r\right)$ כאשר $\alpha_1,\ldots,\alpha_r$ הם שורשי f. בפרט, כל ה-α_i-ספרביליים. הטענה נובעת כעת מתרגיל 14.22. ∎

התרגיל הבא מכליל את מסקנה 14.21:

תרגיל 14.24 הוכיחו כי היחס של הרחבות ספרביליות הוא טרנזיטיבי, גם ללא הנחת סופיות. כלומר, הוכיחו כי אם ${}^{M}\!/_{K}$ ו-${}^{L}\!/_{M}$ הרחבות אלגבריות ספרביליות של שדות, אז גם ${}^{L}\!/_{K}$ ספרבילית.

דוגמאות

דוגמה 14.25 ההרחבה ${}^{\mathbb{C}}\!/_{\mathbb{R}}$ היא הרחבה ספרבילית, כי כל הרחבה אלגברית של שדות ממציין 0 היא ספרבילית. ואכן, $i\left({}^{\mathbb{C}}\!/_{\mathbb{R}}\right)=\left[\mathbb{C}:\mathbb{R}\right]=2$. למשל, אם $\varphi:\mathbb{R}\hookrightarrow\mathbb{C}$ הוא השיכון הסטנדרטי, אז

$$i\left({}^{\mathbb{C}}\!/_{\mathbb{R}}\right)=i_{\varphi}\left({}^{\mathbb{C}}\!/_{\mathbb{R}}\right)=\left|\mathrm{Aut}\left({}^{\mathbb{C}}\!/_{\mathbb{R}}\right)\right|=\left|\{e,\tau\}\right|$$

(כאשר τ הוא אוטומורפיזם ההצמדה — ראו דוגמה 13.12). השוויון $i_\varphi\left(\mathbb{C}/\mathbb{R}\right) = \left|\mathrm{Aut}\left(\mathbb{C}/\mathbb{R}\right)\right|$ נובע מכך שכל שיכון של $\mathbb{C}$ בתוך עצמו שמקבע את $\mathbb{R}$ הוא אוטומורפיזם: זוהי בפרט העתקה לינארית שהיא שיכון של $\mathbb{C}$, מרחב וקטורי מממד 2 מעל $\mathbb{R}$, לתוך עצמו. משיקולי ממד, העתקה כזו חייבת להיות גם על.

דוגמה 14.26 יהי $\alpha = \sqrt[3]{2}$ השורש הממשי של הפולינום $x^3 - 2 \in \mathbb{Q}[x]$ ותהי $L = \mathbb{Q}(\alpha)$ (ראו דוגמה 13.18). ראינו כי $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, ומכיוון שהמציין הוא 0 הרחבה זו ספרבילית, ולכן $i\left(L/\mathbb{Q}\right) = 3$. למשל, אם $\varphi : \mathbb{Q} \hookrightarrow \mathbb{C}$ השיכון הסטנדרטי (והיחידי), אז יש לו שלוש הרחבות אפשריות לשיכונים של L ב-$\mathbb{C}$: השיכון ששולח את α לעצמו, זה ששולח את α ל-$\alpha\omega$ וזה ששולח את α ל-$\alpha\omega^2$ ($\omega = e^{\frac{2\pi i}{3}}$).

דוגמה 14.27 יהיו $K = \mathbb{F}_p(t)$, $f(x) = x^p - t \in K[x]$ ו-L שדה הרחבה של K מממד p שבו יש ל-f שורש α (דוגמה 13.19). ההרחבה L/K היא פשוטה: $L = K(\alpha)$, ו-$f = m_\alpha$. לפי למה 14.18, $i\left(L/K\right) = 1$ כי α הוא השורש היחידי של f.

הערה 14.28 כפי שראינו, הרחבות אלגבריות אי-ספרביליות תתכנה רק אם המציין הוא $p > 0$. ברם, גם לשדה K ממציין p ייתכן שכל הרחבה שלו היא ספרבילית: למשל, אם K סופי (נראה זאת להלן במסקנה 14.31, ושוב במסקנה 17.4), או אם K סגור אלגברית (באופן טריוויאלי). שדה ללא הרחבות אלגבריות אי-ספרביליות נקרא **שדה משוכלל** (perfect field). אם כן, כל שדה ממציין 0 הוא משוכלל. המשפט הבא מספק קריטריון להיותו של שדה ממציין p משוכלל. שדה משוכלל

משפט 14.29 יהי K שדה ממציין p. אזי K משוכלל, כלומר, אין לו הרחבות אלגבריות אי-ספרביליות, אם ורק אם האנדומורפיזם של פרובניוס $\phi : K \to K$, המוגדר על-ידי $\phi(k) = k^p$ (ראו משפט 13.5) הוא גם על, כלומר אוטומורפיזם של K.

למשל, השדה $K = \mathbb{F}_p(t)$ איננו משוכלל: ראינו זה עתה כי יש לו הרחבה אלגברית אי-ספרבילית.

תרגיל 14.30 הוכיחו את המשפט האחרון. הדרכה:

1. הראו שהתנאי במשפט הכרחי: אם K משוכלל, האנדומורפיזם של פרובניוס על.
   רמז: הניחו בשלילה שקיים $\alpha \in K$ ללא שורש מסדר p, והסתכלו בשדה הפיצול של $x^p - \alpha$.
2. הראו כי שדה הוא משוכלל אם ורק אם כל פולינום אי-פריק מעליו הוא ספרבילי.
3. יהי $f \in K[x]$ אי-פריק. הראו שאם f אינו ספרבילי אז הוא מהצורה
   $f = a_n x^{pn} + a_{n-1} x^{p(n-1)} + \ldots + a_1 x^p + a_0$.
4. הניחו כי האנדומורפיזם של פרובניוס הוא על K, וכתבו $a_i = b_i^p$. הראו ש-
   $f = (b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0)^p$, בסתירה להיותו אי-פריק. הסיקו את המשפט.

מסקנה 14.31 שדה סופי הוא משוכלל.

הוכחה: יהי K שדה סופי. אזי הוא בהכרח ממציין ראשוני p. מכיוון שכל פונקציה חח"ע מקבוצה סופית לעצמה היא על, גם האנדומורפיזם של פרובניוס הוא על K. לפי המשפט, K משוכלל. ■

תרגיל 14.32 יהי K שדה ממציין ראשוני p, ויהי $\alpha \in K$ איבר שאין לו שורש מסדר p בתוך K. הוכיחו כי $x^p - \alpha$ הוא פולינום אי-פריק.
הדרכה: יהי β שורש של הפולינום בשדה הרחבה כלשהו. הוכיחו כי הפולינום המינימלי של β מעל K הוא $(x-\beta)^j$ עם $2 \le j \le p$ והתבוננו במקדם של x^{j-1} בפולינום זה.
שימו לב שתרגיל זה מכליל את תרגיל 10.99 שבו הראנו כי $x^p - t \in \mathbb{F}_p(t)[x]$ אי-פריק.

15 נורמליות

15.1 הרחבות נורמליות

בסעיף זה נגדיר בצורה פורמלית את המושג "הרחבה נורמלית", שהוגדר בקצרה בעמוד 230 ושלצד ספרביליות, הוא אחד התנאים להיותה של הרחבת שדות הרחבת גלואה.

הרחבה נורמלית

הגדרה 15.1 הרחבת שדות אלגברית L/K נקראת **נורמלית** אם כל פולינום אי-פריק מעל K עם שורש ב-L מתפצל ב-L (לחלוטין).

לדוגמה, אם L סגור אלגברית אז ההרחבה תמיד נורמלית. אין זה מקרה שהמונח "נורמליות" משמש גם להרחבות מסוג זה וגם לסוג מסוים של תת-חבורות בתורת החבורות. במשפט היסודי של תורת גלואה (משפטים 16.3 ו-16.6) נראה את הקשר העמוק בין שני המושגים הללו.

במקרה של הרחבות **סופיות**, ניתן לבדוק אם הרחבה היא נורמלית גם באמצעות קריטריונים אחרים. אחד מהם מסתמך על ספירת אוטומורפיזמים של ההרחבה. נזכיר כי $\mathrm{Aut}\left(L/K\right)$ הוא חבורת האוטומורפיזמים של השדה L שמקבעים את K. יהי Ω הסגור האלגברי של L, ויהי $\mathrm{id} : K \to \Omega$ שיכון הזהות.

$$\begin{array}{ccc}
\Omega & & \Omega \\
| & & | \\
L & & L \\
| & & | \\
K & \xrightarrow{\mathrm{id}} & K
\end{array}$$

כזכור, מספר הדרכים להרחיב את הזהות על K **לשיכון** של L ב-Ω שווה ל-$i\left(L/K\right)$, אינדקס הספרביליות של L/K. ברור שכל אוטומורפיזם ב-$\mathrm{Aut}\left(L/K\right)$ הוא בפרט שיכון שכזה, ולכן:

טענה 15.2 לכל הרחבה סופית L/K מתקיים

$$\left|\mathrm{Aut}\left(L/K\right)\right| \le i\left(L/K\right).$$

המשפט הבא מספק שני קריטריונים חדשים לנורמליות של הרחבות סופיות:

משפט 15.3 בעבור הרחבת שדות סופית L/K, התנאים הבאים שקולים:
(i) L/K היא נורמלית, כלומר כל פולינום אי-פריק ב-$K[x]$ שיש לו שורש ב-L, מתפצל לחלוטין מעל L.
(ii) $\left|\mathrm{Aut}\left(L/K\right)\right| = i\left(L/K\right)$.
(iii) L הוא שדה פיצול של פולינום כלשהו ב-$K[x]$ (לאו דווקא אי-פריק).

הוכחה: נראה כי $(i) \Longrightarrow (iii) \Longrightarrow (ii) \Longrightarrow (i)$. תחילה נניח כי (i) מתקיים, כלומר L/K נורמלית, ונוכיח כי L הוא שדה פיצול של פולינום ב-$K[x]$, דהיינו את (iii). נכתוב $L = K(\theta_1, \ldots, \theta_m)$. יהי $g_i \in K[x]$ הפולינום המינימלי של θ_i מעל K. מכיוון ש-g_i אי-פריק ויש לו שורש ב-L, הוא מתפצל שם (לחלוטין). לכן המכפלה

$$g = \prod_{i=1}^{m} g_i$$

מתפצלת ב-L (לחלוטין). אבל שורשי g יוצרים את L מעל K, שכן הם כוללים את $\theta_1, \ldots, \theta_m$. לכן L הוא שדה הפיצול של g.

$(iii) \Longleftarrow (ii)$: נניח כי L הוא שדה פיצול של $f \in K[x]$. אם שורשיו השונים של f ב-L הם $\alpha_1, \ldots, \alpha_r$, אזי $L = K(\alpha_1, \ldots, \alpha_r)$. מספר ההרחבות של $\mathrm{id} : K \to K$ לשיכונים של L ב-Ω (הסגור האלגברי של L) הוא $i\left({}^{L}\!/_{K}\right)$. כמובן, כל שיכון φ כזה נקבע ביחידות לפי התמונות של $\alpha_1, \ldots, \alpha_r$. בנוסף, $\varphi(\alpha_i)$ מאפס כל פולינום ש-α_i מאפס, ובפרט הוא שורש של f. לכן $\varphi(\alpha_i) \in \{\alpha_1, \ldots, \alpha_r\} \subseteq L$. לפיכך, כל שיכון $\varphi : L \to \Omega$ שמרחיב את $\mathrm{id} : K \to K$ מקיים

$$\varphi(L) = \varphi(K(\alpha_1, \ldots, \alpha_r)) = K(\varphi(\alpha_1), \ldots, \varphi(\alpha_r)) \subseteq L.$$

כלומר זהו שיכון שתמונתו מוכלת ב-L. אך φ הוא איזומורפיזם בין L לבין התמונה $\varphi(L)$, ולפיכך מתקיים $[L : K] = [\varphi(L) : K]$. על כן $\varphi(L) = L$ וקיבלנו כי כל אחד מהשיכונים שספרנו ב-$i\left({}^{L}\!/_{K}\right)$ הוא שיכון שתמונתו בדיוק L, כלומר אוטומורפיזם של L שמצטמצם לזהות על K. לפיכך

$$\left|\mathrm{Aut}\left({}^{L}\!/_{K}\right)\right| = i\left({}^{L}\!/_{K}\right).$$

$(ii) \Longleftarrow (i)$: לבסוף, נניח כי $\left|\mathrm{Aut}\left({}^{L}\!/_{K}\right)\right| = i\left({}^{L}\!/_{K}\right)$ ונראה כי ${}^{L}\!/_{K}$ נורמלית. נניח בשלילה כי היא אינה נורמלית, כלומר, קיים $\alpha \in L$ כך שהפולינום המינימלי שלו m_α אינו מתפצל ב-L. יהי $\beta \in \Omega \setminus L$ שורש של m_α. כפי שראינו בהוכחה של למה 14.18, יש שיכון של $K(\alpha)$ בתוך Ω שמקבע את K ושולח את α אל β. אם נרחיב שיכון זה לשיכון של L כולו, ברור כי נקבל שיכון של L ב-Ω שתמונתו אינה מוכלת ב-L, ולכן הוא איננו אוטומורפיזם של L. לפיכך, במקרה זה נקבל אי-שוויון חזק

$$\left|\mathrm{Aut}\left({}^{L}\!/_{K}\right)\right| < i\left({}^{L}\!/_{K}\right).$$

■

מסקנה 15.4 אם ${}^{L}\!/_{K}$ הרחבה נורמלית סופית ו-M שדה ביניים, אז גם ${}^{L}\!/_{M}$ הרחבה נורמלית.

הוכחה: השדה L הוא שדה הפיצול מעל K של איזה פולינום $f \in K[x]$. בפרט, $f \in M[x]$ ו-L הוא בהכרח גם שדה הפיצול של f מעל M. לכן ${}^{L}\!/_{M}$ נורמלית. ■

תרגיל 15.5 הכלילו את השקילות בין סעיפים (i) ו-(ii) ממשפט 15.3 למקרה של הרחבות אלגבריות אינסופיות:
כל $\sigma \in \mathrm{Aut}\left({}^{L}\!/_{K}\right)$ הוא בפרט הרחבה של $\mathrm{id} : K \to K$ לשיכון של L בתוך Ω, הסגור האלגברי של L. הראו כי ${}^{L}\!/_{K}$ נורמלית אם ורק אם שתי הקבוצות הללו זהות, כלומר כל שיכון של L בתוך Ω שמרחיב את הזהות על K הוא למעשה אוטומורפיזם של ${}^{L}\!/_{K}$.

תרגיל 15.6 יהי $L \supseteq M \supseteq K$ מגדל של שדות, כך ש-${}^{M}\!/_{K}$ נורמלית. הוכיחו כי לכל $\sigma \in \mathrm{Aut}\left({}^{L}\!/_{K}\right)$,

$$\sigma(M) = M.$$

כלומר, תת-הרחבות נורמליות נשמרות תחת אוטומורפיזמים של הרחבות. שימו לב שהעובדה ש-$\sigma(M) = M$ כקבוצה אינה גוררת ש-$\sigma|_M$ היא הזהות, כלומר אינה גוררת ש- מקבעת את M.

תרגיל 15.7 יהי $L \supseteq M \supseteq K$ מגדל של הרחבות אלגבריות של שדות (לאו דווקא סופיות). הוכיחו או הפריכו את הטענות הבאות. (השוו עם התרגילים המקבילים בעבור תכונת הספרביליות: תרגילים 14.15 ו-14.24).

1. אם L/K נורמלית, גם M/K נורמלית.
2. אם L/K נורמלית, גם L/M נורמלית.
3. אם M/K ו-L/M נורמליות, גם L/K נורמלית.

15.2 הרחבות גלואה

לאחר שהגדרנו באופן מסודר מתי הרחבה נקראת ספרבילית ומתי היא נקראת נורמלית, ניתן לנסח באופן פורמלי גם מהי הרחבת גלואה:

הרחבת גלואה

הגדרה 15.8 הרחבת שדות אלגברית נקראת **הרחבת גלואה** אם היא ספרבילית ונורמלית.
אם L/K הרחבת גלואה, חבורת האוטומורפיזמים $\mathrm{Aut}\left(L/K\right)$ נקראת **חבורת גלואה** (של ההרחבה) ומסומנת גם $\mathrm{Gal}\left(L/K\right)$.

$\mathrm{Gal}\left(L/K\right)$

המשפט הבא מסכם כמה קריטריונים שדי בכל אחד מהם על מנת לקבוע אם הרחבת שדות **סופית** היא גלואה:

משפט 15.9 בעבור הרחבת שדות סופית L/K, התנאים הבאים שקולים:
(i) L/K היא גלואה, כלומר נורמלית וספרבילית.
(ii) $\left|\mathrm{Aut}\left(L/K\right)\right| = [L:K]$.
(iii) L הוא שדה פיצול של פולינום **ספרבילי** מ-$K[x]$ (לאו דווקא אי-פריק).

הוכחה: ההוכחה תהיה בעיקרה קיבוץ של טענות שכבר הוכחנו. תחילה נסביר מדוע $(ii) \iff (i)$.
ממשפט 15.3 בצירוף משפט 14.20, נקבל כי

$$1 \le \left|\mathrm{Aut}\left(L/K\right)\right| \overset{(\text{ב})}{\le} i\left(L/K\right) \overset{(\text{א})}{\le} [L:K] \tag{16}$$

כאשר ב-(א) יש שוויון אם ורק אם ההרחבה L/K ספרבילית, וב-(ב) יש שוויון אם ורק אם L/K נורמלית.
לכן $\left|\mathrm{Aut}\left(L/K\right)\right| = [L:K]$ אם ורק אם L/K גלואה (ואחרת $\left|\mathrm{Aut}\left(L/K\right)\right| < [L:K]$).

כעת נראה כי $(i) \Longrightarrow (iii)$. מכך ש-$L/K$ גלואה נובע בפרט שהיא נורמלית ולכן L הוא שדה פיצול של איזה פולינום $f \in K[x]$. נניח כי הפירוק של f לגורמים אי-פריקים הוא $f = f_1 f_2 \cdots f_r$. בלי הגבלת הכלליות, ניתן להניח כי ה-f_i-ים מתוקנים ושונים זה מזה: שדה הפיצול של פולינום אינו משתנה אם משמיטים עותקים כפולים של גורמים אי-פריקים בו. נטען כי f הוא פולינום ספרבילי. לפולינומים f_i ו-f_j אין שורשים משותפים (אם $i \neq j$), שהרי הם אי-פריקים ושונים ולכן $(f_i, f_j) = 1$ וכזכור, ה-gcd של פולינומים אינו תלוי בשדה שבו נעשה החישוב (טענה 14.5).

נותר להראות שאם $\alpha \in L$ שורש של f_i, הוא שורש פשוט של f_i. מכיוון ש-f_i אי-פריק (ומתוקן), הוא הפולינום המינימלי של α מעל K. אבל L/K ספרבילית, ובפרט α ספרבילי, ולכן הפולינום המינימלי שלו, f_i, הוא ספרבילי ו-α שורש פשוט שלו.

לבסוף, הגרירה $(iii) \Longrightarrow (i)$ נובעת מכך שאם L הוא שדה פיצול של פולינום **ספרבילי** מ-$K[x]$ אז L/K נורמלית לפי משפט 15.3, וספרבילית לפי משפטון 14.23. ■

במסקנה 16.2 שבפרק הבא נוסיף על שלושת התנאים הללו תנאי שקול רביעי. כמסקנה נוספת מהדיון שלנו בהרחבות ספרביליות ובהרחבות נורמליות, מתקיים:

מסקנה 15.10 אם L/K הרחבת גלואה סופית ו-M שדה ביניים, אז גם L/M גלואה.

הוכחה: הטענה נובעת מהתוצאות המקבילות בעבור הרחבות ספרביליות (תרגיל 14.15) ובעבור הרחבות נורמליות (מסקנה 15.4). ■

תרגיל 15.11 יהי $K \subseteq M \subseteq L$ מגדל של הרחבות אלגבריות של שדות (לאו דווקא סופיות). הוכיחו את הטענות הבאות. (השוו עם תרגילים 14.15 ו-14.24 בעבור תכונת הספרביליות ועם תרגיל 15.7 בעבור תכונת הנורמליות.)

1. הראו כי גם אם L/K גלואה, M/K לאו דווקא גלואה.
2. הראו כי אם L/K גלואה, גם L/M גלואה.
3. הראו כי גם אם M/K ו-L/M גלואה, L/K לאו דווקא גלואה.

15.3 עוד על שדות פיצול

ראינו כי כל הרחבה נורמלית סופית היא, למעשה, שדה פיצול של פולינום. לסיום פרק זה נדון במספר תכונות של שדות פיצול בעלות חשיבות משל עצמן. נזכיר כי בהינתן שדה K ופולינום $f \in K[x]$, שדה פיצול של f מעל K הוא הרחבה L של K שבה f מתפצל, כך שאין שדה ביניים שמוכל ממש ב-L שבו f מתפצל. את קיומו של שדה פיצול ניתן לגזור מקיומו של סגור אלגברי $\overline{K}$ של K: הרי f מתפצל ב-$\overline{K}$, ואז תת-השדה שנוצר על-ידי שורשיו הוא שדה פיצול. המשפט הבא מראה שתמיד קיים שדה פיצול מממד הרחבה החסום על-ידי $n!$, כאשר n היא מעלת הפולינום. יתר על כן, הוכחת המשפט מספקת הוכחה ישירה לקיומו של שדה פיצול, ללא שימוש בעובדה הקשה יותר של קיום סגור אלגברי. לאחר מכן (משפט 15.15) נראה, בנוסף, ששדה פיצול הוא יחיד עד כדי איזומורפיזם (או אז נוכל לקרוא לו **שדה הפיצול**, ביידוע).

משפט 15.12 לכל $f \in K[x]$ ממעלה n יש שדה פיצול שדרגת ההרחבה שלו לכל היותר $n!$.

הוכחה: ההוכחה באינדוקציה על n. בעבור $n = 0$ או $n = 1$ מובן כי K, ורק K, הוא שדה הפיצול של f וטענת המשפט מתקיימת טריוויאלית. כעת נניח כי $\deg f = n$ וכי טענת המשפט נכונה לכל מספר הקטן מ-n. כפי שראינו (במשפט 11.35), יש שדה הרחבה E/K שבו יש ל-f שורש ומתקיים $[E:K] \leq n$. יהי $\alpha \in E$ שורש של f. בתוך $E[x]$, f מתפרק כ-$f(x) = g(x)(x-\alpha)$ בעבור איזה $g \in E[x]$ ממעלה $n-1$. לפי הנחת האינדוקציה, קיים שדה הרחבה L של E שהוא שדה פיצול של g, עם $[L:E] \leq (n-1)!$. בפרט, $L = E(\alpha_2, \ldots, \alpha_n)$, כאשר $\alpha_2, \ldots, \alpha_n$ הם שורשי g (והם לאו דווקא שונים זה מזה). לפיכך f מתפצל ב-L, ו-

$$K(\alpha, \alpha_2, \ldots, \alpha_n) \subseteq L$$

הוא שדה פיצול שלו. לבסוף,

$$[K(\alpha, \alpha_2, \ldots, \alpha_n) : K] \leq [L:K] = [L:E][E:K] \leq (n-1)! \cdot n = n! \,.$$

■

תרגיל 15.13

1. בהוכחה הראינו רק כי קיים שדה פיצול מדרגת הרחבה לכל היותר $n!$. הוכיחו כי כל שדה פיצול L של f מקיים $[L:K] \leq n!$.
2. הוכיחו כי, יתר על כן, אם L שדה פיצול של f מעל K אז $[L:K] \mid n!$.
3. הוכיחו כי אם הפירוק של f לגורמים אי-פריקים הוא $f = f_1 \cdots f_r$ עם $\deg f_i = n_i$ אזי דרגת שדה פיצול של f חסומה על-ידי $n_1! n_2! \cdots n_r!$.

דוגמאות

- בהמשך לדוגמה 13.28, לפולינום המינימלי של $\zeta = e^{\frac{2\pi i}{p}}$, שורש היחידה מסדר p, יש שדה פיצול $L = \mathbb{Q}(\zeta)$ שמכיל כבר את כל שורשי הפולינום, הלוא הם $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. מתקיים $[L : \mathbb{Q}] = p - 1$ (ושימו לב שזה מספר קטן בהרבה מהחסם $(p-1)!$ שראינו במשפט 15.12).
- בדוגמה 13.33, נתקלנו בשדה פיצול של הפולינום $x^3 - 2 \in \mathbb{Q}[x]$. שדה הפיצול היה $L = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$, ומתקיים $[L : \mathbb{Q}] = 6 = 3!$.
- השדה $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ הוא שדה פיצול של $f(x) = (x^2-2)(x^2-3)$ (נתקלנו בו בסעיף 13.4). כאן $[L : \mathbb{Q}] = 4 < 4!$ (והשוו עם סעיף 3 בתרגיל 15.13).

תרגיל 15.14 היזכרו בדוגמה 13.33.

1. כתבו את הפירוק של $x^3 - 2$ ב-$\mathbb{Q}(\alpha)[x]$ (כאשר $\alpha = \sqrt[3]{2}$ השורש השלישי הממשי של 2).
2. הוכיחו כי אותו L, תת-השדה של $\mathbb{C}$ שהוא שדה פיצול של $x^3 - 2$ מעל $\mathbb{Q}$, הוא גם שדה פיצול של $x^3 - 3x^2 + 3x - 3 = (x-1)^3 - 2$.
   כלומר, אותו שדה הרחבה עשוי להיות שדה פיצול של פולינומים שונים.

משפט 15.15 שדה הפיצול של פולינום $f \in K[x]$ הוא יחיד עד כדי איזומורפיזם.

נעיר שכאשר מדובר על איזומורפיזם של שדות פיצול הכוונה היא לאיזומורפיזם בין השדות שמקבע את תת-השדה K (שמוכל בשניהם).

הוכחת משפט 15.15: יהיו L_1 ו-L_2 שני שדות פיצול של f מעל K, ויהי Ω הסגור האלגברי של L_2. נרחיב את השיכון הטריוויאלי $\mathrm{id} : K \hookrightarrow \Omega$ של K ב-Ω לשיכון $\varphi : L_1 \hookrightarrow \Omega$ של L_1 כולו. כמובן, φ משרה איזומורפיזם בין L_1 ל-$L_1' = \varphi(L_1)$ (איזומורפיזם שמקבע את K), ולכן גם L_1' שדה פיצול של f מעל K.

$$\begin{tikzcd}
 & \Omega \arrow[d, dash] \arrow[dr, dash] & \\
L_1 \arrow[r, hook, dotted, "\varphi"] \arrow[d, dash] & L_1' \arrow[d, dash] & L_2 \arrow[dl, dash] \\
K \arrow[r, "\mathrm{id}"] & K &
\end{tikzcd}$$

אבל מהיות L_1' ו-L_2 שדות פיצול של הפולינום $f \in K[x]$, נובע כי שניהם נוצרים מ-K על-ידי שורשי f בתוך Ω. לכן $L_1' = L_2$, והשיכון φ תמונתו, למעשה, L_2. לפיכך L_1 ו-L_2 שדות פיצול איזומורפיים. ■