13 מבוא לתורת גלואה

תורת גלואה עוסקת בהרחבות סופיות של שדות. בפרק הקודם ראינו כיצד כבר מנקודת המבט שרואה את ההרחבה L/K כמרחב וקטורי ממימד $[L:K]$, ניתן להסיק מסקנות משמעותיות לגבי אי-היתכנות של בניות מסוימות בסרגל ובמחוגה. עם זאת, נקודת מבט זו אינה לוקחת בחשבון את המבנה העשיר של L כשדה. במוחו של אווריסט גלואה (Évariste Galois) עלה הרעיון המבריק להתאים לכל הרחבה שדות L/K **חבורה** שבנסיבות מסוימות ניתן ללמוד ממנה רבות על ההרחבה: למשל, מהן כל תת-ההרחבות (שדות הביניים) וכיצד הן מוכלות זו בזו. רעיון זה מעורר השתאות עוד יותר כאשר לוקחים בחשבון שבזמנו של גלואה (המחצית הראשונה של המאה ה-19) המושג המופשט של חבורה טרם הוגדר. למעשה, תורת גלואה הייתה מן הגורמים המאיצים העיקריים לפיתוחה של תורת החבורות.

13.1 חבורת האוטומורפיזמים של שדה

החבורה שהגדיר גלואה קשורה לחבורת האוטומורפיזמים של שדה. נזכיר כי אוטומורפיזם של שדה L הוא איזומורפיזם של שדות מ-L לעצמו[1]. חבורת האוטומורפיזמים של שדה L היא

$\boxed{\operatorname{Aut}(L)}$

$$\operatorname{Aut}(L)=\{\sigma:L\to L \mid \sigma \text{ הוא אוטומורפיזם}\}.$$

כלומר, איברי החבורה הם האוטומורפיזמים של L, והפעולה בחבורה היא הרכבת אוטומורפיזמים.

טענה 13.1 $\operatorname{Aut}(L)$ היא אמנם חבורה.

תרגיל 13.2 הוכיחו טענה זאת. עליכם:

(i) להסביר מדוע ההרכבה היא פעולה בינארית על הקבוצה $\operatorname{Aut}(L)$, כלומר מדוע הרכבה של שני אוטומורפיזמים נותנת אוטומורפיזם.

(ii) להסביר מדוע ההרכבה היא פעולה אסוציאטיבית.

(iii) להצביע על איבר היחידה ולהוכיח שהוא אמנם יחידה.

(iv) להראות שלכל איבר יש הפכי.

בכל שדה יש לפחות אוטומורפיזם אחד, טריוויאלי: אוטומורפיזם הזהות e. לעתים אין אוטומורפיזמים נוספים:

תרגיל 13.3 הוכיחו כי $\operatorname{Aut}(L)$ היא חבורה טריוויאלית כאשר L הוא

1. $\mathbb{Q}$
2. $\mathbb{F}_p$ (שדה מסדר ראשוני p; השוו ל-$\operatorname{Aut}(\mathbb{Z}_p)$, חבורת האוטומורפיזמים של החבורה החיבורית של $\mathbb{F}_p$, שחקרנו בפרק 1.5).
3. $\mathbb{R}$ (שימו לב שאיננו מניחים כאן כל הנחה לגבי רציפות האוטומורפיזמים.)

רמז: הראו שאוטומורפיזם מעביר ריבוע לריבוע, כלומר, לכל $x\in\mathbb{R}$ קיים $y\in\mathbb{R}$ כך שהאוטומורפיזם מעביר את x^2 ל-y^2.

תרגיל 13.4 יהי L שדה. היזכרו בהגדרה של "תת-השדה הראשוני" של L (במסגרת טענה 10.86).

1. יהי $\theta\in\operatorname{Aut}(L)$. הוכיחו כי הצמצום של θ לשדה הראשוני של L הוא הזהות.
2. תארו את $\operatorname{Aut}\left(\mathbb{Q}\left(\sqrt{2}\right)\right)$.

[1] וראו עמוד 192.

המשפט הבא מתאר אנדומורפיזם[2] בעל חשיבות בשדות ממציין ראשוני, שלעתים קרובות הוא אף אוטומורפיזם:

משפט 13.5 יהי L שדה ממציין p, ותהי $\phi : L \to L$ ההעתקה המוגדרת על-ידי $\phi(x) = x^p$. אזי ϕ היא שיכון, כלומר הומומורפיזם חח״ע מ-L לעצמו.
שיכון זה נקרא **האנדומורפיזם של פרובניוס**.

האנדומורפיזם של פרובניוס

לצורך הוכחת המשפט נזכיר עובדה מתמטית חשובה[3]:

למה 13.6 יהיו p מספר ראשוני ו-k מספר טבעי המקיים $1 \le k \le p-1$. אזי $p|\binom{p}{k}$.

הוכחת למה 13.6: מתקיים $\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$. המקדם הבינומי הוא מספר שלם, ועל כן כל הגורמים הראשוניים שבמכנה מצטמצמים עם גורמים מתאימים במונה. מאידך, ברור כי הראשוני p אינו גורם במכנה אבל דווקא כן גורם במונה, ולכן הוא שורד גם לאחד הצמצומים. ■

הוכחת משפט 13.5: נראה תחילה ש-ϕ היא הומומורפיזם של שדות. ברור כי היא מקבעת את איבר היחידה וכי היא משמרת את הכפל שהרי $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\cdot\phi(y)$. מכיוון שהשדה L ממציין p, מתקיים, לפי הלמה, שבתוך השדה $\binom{p}{k} = 0$ לכל $1 \le k \le p-1$. לפיכך,

$$\begin{aligned}\phi(x+y) &= (x+y)^p \\ &= \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \ldots + \binom{p}{p-1}xy^{p-1} + \binom{p}{p}y^p \\ &= x^p + y^p \\ &= \phi(x) + \phi(y)\end{aligned}$$

קיבלנו כי ϕ משמרת גם את החיבור. נותר להראות כי ϕ חח״ע, אך זה נובע מהעובדה הכללית שכל הומומורפיזם של שדות הוא שיכון (ראו תרגיל 9.20). ■

תרגיל 13.7

1. הוכיחו כי אם L שדה סופי ממציין p אז $\phi \in \mathrm{Aut}(L)$.
2. תנו דוגמה לשדה (ממציין p) שבו φ אינו על (ועל כן אינו אוטומורפיזם).

תרגיל 13.8 הוכיחו כי התכונה של מספר ראשוני p שמתוארת בלמה 13.6 היא ייחודית לראשוניים. כלומר, הראו שמספר טבעי $n \ge 2$ מקיים $n \mid \binom{n}{k}$ לכל $1 \le k \le n-1$ אם ורק אם n ראשוני.
הערה: במשך מספר עשורים, אתגר ידוע במתמטיקה בכלל ובתחום ההצפנות בפרט היה למצוא אלגוריתם יעיל שמסוגל להכריע בוודאות אם מספר נתון, גדול מאוד, הוא ראשוני אם לאו[4]. רק בשנת 2002, לראשונה, המציאו שלושה חוקרים הודים – Manindra Agrawal, Neeraj Kayal ו-Nitin Saxena – אלגוריתם שסיפק את ציפיות הקהילה המתמטית. האפיון של הראשוניים שאתם מתבקשים להוכיח כאן מהווה נדבך מרכזי באלגוריתם זה.

[2] נזכיר כי אנדומורפיזם הוא הומומורפיזם ממבנה אלגברי לעצמו (ראו, למשל, עמוד 146).
[3] למעשה, נתקלנו כבר בעובדה זו במסגרת דוגמה 10.103.
[4] בניגוד לאלגוריתמים וודאיים, או דטרמיניסטיים, אלגוריתמים הסתברותיים יעילים לבדיקת ראשוניות ידועים היו זמן רב קודם לכן - ראו הערת שוליים בעמוד 184. אלגוריתם הסתברותי לרוב מספק את התשובה הנכונה בהסתברות גדולה מאוד (הקרובה כרצוננו להסתברות 1), אך לא בוודאות מוחלטת.

13.2 חבורת האוטומורפיזמים של הרחבת שדות

תהי $^L/_K$ הרחבת שדות כלשהי. החבורה שהגדיר גלואה בעבור הרחבה זו היא תת-חבורה של $\mathrm{Aut}\,(L)$ המורכבת מהאוטומורפיזמים שצמצומם ל-K הוא הזהות, כלומר אלו שמקבעים[5] את איברי K:

$\mathrm{Aut}\,(^L/_K)$

הגדרה 13.9 חבורת האוטומורפיזמים של ההרחבה $^L/_K$ היא

$$\mathrm{Aut}\,(^L/_K) = \{\sigma \in \mathrm{Aut}\,(L) \mid \sigma\,(x) = x \ \ \forall x \in K\}.$$

תרגיל 13.10 הוכיחו כי אמנם $\mathrm{Aut}\,(^L/_K) \leq \mathrm{Aut}\,(L)$ (כלומר, הראו שזו תת-חבורה).

דוגמה 13.11 אם K הוא השדה הראשוני של L, אז $\mathrm{Aut}\,(^L/_K) = \mathrm{Aut}\,(L)$. (ראו תרגיל 13.4.)

דוגמה 13.12 החבורה המתאימה להרחבה $^\mathbb{C}/_\mathbb{R}$ היא $\mathrm{Aut}\,(^\mathbb{C}/_\mathbb{R}) = \{e, \tau\}$ כאשר τ הוא אוטומורפיזם ההצמדה: $\tau\,(z) = \overline{z}$. אכן, τ הוא אוטומורפיזם אשר מקבע את הממשיים. מצד שני, אם $\sigma \in \mathrm{Aut}\,(^\mathbb{C}/_\mathbb{R})$ אז

$$\sigma\,(i)^2 = \sigma\left(i^2\right) = \sigma\,(-1) = -1$$

ולפיכך $\sigma\,(i) \in \{\pm i\}$. אם $\sigma\,(i) = -i$ מקבלים את אוטומורפיזם ההצמדה שכן לכל $a, b \in \mathbb{R}$, מתקיים

$$\sigma\,(a + ib) = \sigma\,(a) + \sigma\,(i)\,\sigma\,(b) = a - ib.$$

אם $\sigma\,(i) = i$, נקבל באותו אופן את אוטומורפיזם הזהות. לכן אלו שני האוטומורפיזמים היחידים של $\mathbb{C}$ שמקבעים את[6] $\mathbb{R}$. כמובן, $\mathrm{Aut}\,(^\mathbb{C}/_\mathbb{R}) \cong \mathbb{Z}_2$.

תרגיל 13.13 יהי $\mathbb{R}\,(t)$ שדה הפונקציות הרציונליות במשתנה t מעל $\mathbb{R}$.

1. הוכיחו כי לכל $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2\,(\mathbb{R})$ יש אוטומורפיזם יחיד $\sigma_g \in \mathrm{Aut}\,(^{\mathbb{R}(t)}/_\mathbb{R})$ שמקיים

$$\sigma_g\,(t) = \frac{at + c}{bt + d}.$$

2. הוכיחו כי $\sigma_g \circ \sigma_h = \sigma_{gh}$, כלומר הראו כי

$$\varphi : \mathrm{GL}_2\,(\mathbb{R}) \to \mathrm{Aut}\,(^{\mathbb{R}(t)}/_\mathbb{R}) \qquad \varphi\,(g) = \sigma_g$$

הוא הומומורפיזם של חבורות.

3. מהו $\ker\varphi$?

הערה: ניתן להראות, אם כי אין זה טריוויאלי, ש-φ הוא על, כלומר שכל אוטומורפיזם של $\mathbb{R}\,(t)$ שמקבע את $\mathbb{R}$ הוא מהצורה σ_g. מכאן נובע כי $\mathrm{Aut}\,(^{\mathbb{R}(t)}/_\mathbb{R}) \cong \mathrm{GL}_2\,(\mathbb{R}) \,/\, \ker\varphi$.

בשני תת-הסעיפים הבאים נחקור את חבורת האוטומורפיזמים של הרחבות מסוג מיוחד:

---

[5] תהי A קבוצה ו-$B \subseteq A$ תת-קבוצה. כאשר אנו כותבים שהעתקה מהקבוצה A לעצמה **מקבעת** את B, הכוונה שהיא שולחת כל איבר של B לעצמו. כאשר אנו כותבים שהיא **משמרת** את B, הכוונה שהיא שולחת כל איבר של B לתוך B, כלומר, לאיבר כלשהו של B, אך לאו דווקא לעצמו.

[6] מעניין לציין שהחבורה $\mathrm{Aut}\,(\mathbb{C})$ היא אינסופית ואף לא בת מניה (לפחות בהנחת אקסיומת הבחירה). זאת בעוד ש-$\mathrm{Aut}\,(\mathbb{R})$ טריוויאלית ו-$\mathrm{Aut}\,(^\mathbb{C}/_\mathbb{R})$ היא בגודל 2! לקריאה נוספת, ניתן להסתכל במאמר Automorphisms of the Complex Numbers מאת Paul B. Yale בכתב העת Mathematics Magazin, כרך 39, מספר 3, עמודים 135-141.

13.2.1 חבורת האוטומורפיזמים של הרחבות אלגבריות פשוטות

למה 13.14 תהי $L = K(\alpha)$ הרחבת שדות פשוטה. כל $\sigma \in \mathrm{Aut}\left({}^{L}\!/\!{}_{K}\right)$ נקבע לחלוטין על-ידי $\sigma(\alpha)$.

הוכחה: יהי $\sigma \in \mathrm{Aut}\left({}^{L}\!/\!{}_{K}\right)$. כפי שראינו בתרגיל 11.11, איברי ההרחבה $L = K(\alpha)$ הם כולם פונקציות רציונליות ב-α עם מקדמים מ-K. יהי $x \in L$ איבר כלשהו, ונניח שהוא שווה ל-$\frac{c_n\alpha^n+\ldots+c_1\alpha+c_0}{d_m\alpha^m+\ldots+d_1\alpha+d_0}$ עם $c_0,\ldots,c_n,d_0,\ldots,d_m \in K$. מכיוון ש-$\sigma$ מקבע את איברי K (לפי הגדרת $\mathrm{Aut}\left({}^{L}\!/\!{}_{K}\right)$), נקבל כי

$$\sigma(x) = \sigma\left(\frac{c_n\alpha^n+\ldots+c_1\alpha+c_0}{d_m\alpha^m+\ldots+d_1\alpha+d_0}\right) = \frac{c_n(\sigma(\alpha))^n+\ldots+c_1(\sigma(\alpha))+c_0}{d_m(\sigma(\alpha))^m+\ldots+d_1(\sigma(\alpha))+d_0},$$

כך ש-$\sigma(x)$ אכן נקבע מתוך $\sigma(\alpha)$. ■

כעת נניח, בנוסף, שההרחבה הפשוטה היא אלגברית:

למה 13.15 תהי $L = K(\alpha)$ הרחבת שדות אלגברית פשוטה, ויהי $m_\alpha \in K[x]$ הפולינום המינימלי של α מעל K.

1. לכל $\sigma \in \mathrm{Aut}\left({}^{L}\!/\!{}_{K}\right)$, התמונה $\sigma(\alpha)$ היא שורש מתוך L של הפולינום המינימלי m_α.
2. לכל שורש β של m_α ב-L ישנו $\sigma \in \mathrm{Aut}\left({}^{L}\!/\!{}_{K}\right)$ אחד ויחיד שמקיים $\sigma(\alpha) = \beta$.

הוכחה: נניח כי $m_\alpha = c_nx^n+\ldots+c_0 \in K[x]$. מכיוון ש-$\sigma$ מקבע את איברי K נקבל כי

$$m_\alpha(\sigma(\alpha)) = c_n\cdot(\sigma(\alpha))^n+\ldots+c_1\cdot\sigma(\alpha)+c_0 = \sigma(c_n\alpha^n+\ldots+c_1\alpha+c_0) = \sigma(0) = 0,$$

כלומר, $\sigma(\alpha)$ הוא שורש של m_α.

כעת, יהי $\beta \in L$ שורש של m_α. מכיוון ש-m_α אי-פריק (מעל K), הוא הפולינום המינימלי מעל K גם של β. זכרו כי $K[x]/(m_\alpha)$ הוא שדה שאיבריו הם המחלקות של (m_α) בתוך החבורה החיבורית של $K[x]$, וכי סימנו את המחלקה של הפולינום f, כלומר את $f+(m_\alpha)$, בסימון $\overline{f}$. תת-השדה של $K[x]/(m_\alpha)$ שמורכב מהמחלקות של הפולינומים הקבועים ($\{\overline{c}\mid c\in K\}$) איזומורפי ל-$K$ באופן קאנוני, ולכן ניתן לזהותו עם K. לפי טענה 11.20, ישנו איזומורפיזם $K(\beta)\cong K[x]/(m_\alpha)$ ששולח את $\overline{x}$ ל-β ושמקבע את איברי K. (האיזומורפיזם שבנינו בהוכחת טענה 11.20 שולח את $\overline{c}$ ל-c.) באותו אופן ישנו איזומורפיזם $K(\alpha)\cong K[x]/(m_\alpha)$ ששולח את $\overline{x}$ ל-α ומקבע את איברי K. מתוך שרשרת זו של שני האיזומורפיזמים

$$L = K(\alpha) \cong K[x]/(m_\alpha) \cong K(\beta) \subseteq L$$

קיבלנו שקיים איזומורפיזם $\sigma : K(\alpha) \xrightarrow{\cong} K(\beta)$ שמקבע את איברי K ושולח את α ל-β. מאידך, $\beta \in L$ ולכן $K(\beta)\subseteq L$. כלומר $\sigma : L \to L$ הוא שיכון. נותר להראות ש-σ הוא על L. כמובן, σ הוא איזומורפיזם בין L לבין תמונתו $\sigma(L)$. בפרט, $[\sigma(L):K] = [\sigma(L):\sigma(K)] = [L:K]$. מתכונת הכפליות של דרגות הרחבה נובע כי $[L:\sigma(L)] = 1$, כלומר $L = \sigma(L)$, ולכן $\sigma \in \mathrm{Aut}\left({}^{L}\!/\!{}_{K}\right)$. ■

מסקנה 13.16 בהרחבה אלגברית פשוטה ${}^{K(\alpha)}\!/\!{}_{K}$, האוטומורפיזמים הם בהתאמה חח"ע עם שורשי הפולינום המינימלי m_α שנמצאים ב-L.

בהרחבת שדות כלשהי ${}^{E}\!/\!{}_{F}$, אם $f \in F[x]$ פולינום ממעלה n, נאמר כי הוא **מתפצל** מעל E אם פולינום מתפצל

$$f = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \in E[x]$$

(עם $c \in F$ ו-$\alpha_1,\ldots,\alpha_n \in E$, כמובן). השורשים $\alpha_1,\ldots,\alpha_n$ לאו דווקא שונים, ולכן גם אם f מתפצל מעל E ייתכן שיש לו שם פחות מ-n שורשים. מצד שני, אם ל-f יש n שורשים שונים ב-E, ברור כי הוא מתפצל מעליו. מכיוון שמספר השורשים של m_α ב-$L = K(\alpha)$ חסום על-ידי מעלתו, כלומר על-ידי $[L:K]$, נסיק:

מסקנה 13.17 בהרחבה אלגברית פשוטה L/K מתקיים $\left|\operatorname{Aut}\left(L/K\right)\right| \le [L:K]$ ושוויון קיים אם ורק אם הפולינום המינימלי m_α מתפצל לגורמים לינאריים **שונים** ב-L.

למשל, את דוגמה 13.12, שבה ניתחנו את $\operatorname{Aut}\left(\mathbb{C}/\mathbb{R}\right)$, אפשר לנתח גם לאור המסקנות האחרונות. אכן, $\mathbb{C} = \mathbb{R}(i)$, והפולינום המינימלי של i מעל $\mathbb{R}$ הוא, כמובן, x^2+1, שמתפצל לשני גורמים שונים מעל $\mathbb{C}$: $x^2+1 = (x+i)(x-i)$. לפיכך, יש בדיוק שני אוטומורפיזמים ב-$\operatorname{Aut}\left(\mathbb{C}/\mathbb{R}\right)$, אחד ששולח את i לעצמו (ואז מקבלים את הזהות) ואחד ששולח את i ל-$-i$, ואז מקבלים את אוטומורפיזם ההצמדה המרוכבת.

דוגמה 13.18 יהי $\alpha = \sqrt[3]{2}$ השורש הממשי של הפולינום $x^3 - 2 \in \mathbb{Q}[x]$. פולינום זה אי-פריק (למשל, לפי קריטריון אייזנשטיין), ולפיכך זהו הפולינום המינימלי של α מעל $\mathbb{Q}$ וכן $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$. אולם, $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, ול-2 יש רק שורש שלישי ממשי אחד (שני השורשים האחרים הם מרוכבים לא ממשיים). לכן אין לפולינום x^3-2 שורשים נוספים על α בתוך ההרחבה $\mathbb{Q}(\alpha)$. מכאן שהחבורה $\operatorname{Aut}\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right)$ היא טריוויאלית.

דוגמה 13.19 גם בדוגמה זו ניווכח שחבורת האוטומורפיזמים היא טריוויאלית. יהי $K = \mathbb{F}_p(t)$, שדה הפונקציות הרציונליות במשתנה אחד מעל השדה בן p האיברים. בתרגיל 10.106 ראיתם כי הפולינום

$$x^p - t \in K[x]$$

הוא אי-פריק מעל K. יהי α שורש של פולינום זה בסגור האלגברי של K, ויהי $L = K(\alpha)$. שימו לב כי

$$L = K(\alpha) = \mathbb{F}_p(t,\alpha) = \mathbb{F}_p(\alpha),$$

כאשר השוויון האחרון נובע מכך ש-t הוא חזקה של α (בתוך L מתקיים $\alpha^p = t$). מכיוון ש-α הוא טרנסצנדנטי מעל $\mathbb{F}_p$ (לו היה אלגברי, גם t היה אלגברי מעל $\mathbb{F}_p$, בסתירה), L שווה לשדה הפונקציות הרציונליות במשתנה α מעל $\mathbb{F}_p$ (ולפיכך איזומורפי ל-K).

כרגיל, דרגת הרחבה אלגברית פשוטה שווה למעלת הפולינום המינימלי (טענה 11.20), ולפיכך

$$[L:K] = \deg\left(x^p - t\right) = p.$$

אולם, במקרה זה, כל השורשים של הפולינום המינימלי של α הם זהים (ושווים ל-α). זה נובע מכך שבשדות ממציין p, האנדומורפיזם של פרובניוס שמוגדר על-ידי $x \mapsto x^p$ הוא חח״ע (ראו משפט 13.5), ולפיכך אם $\beta \in L$ מקיים $\beta^p - t = 0$ אז $\alpha^p = \beta^p$ ולכן $\alpha = \beta$. לפיכך, לפולינום המינימלי של α יש רק שורש אחד בשדה L, והחבורה $\operatorname{Aut}\left(L/K\right)$ היא טריוויאלית (מכילה רק את אוטומורפיזם הזהות).

תרגיל 13.20 נניח כי $L = K(\alpha)$ הרחבה אלגברית פשוטה וכי הפולינום המינימלי $m_\alpha \in K[x]$ מתפצל לחלוטין לגורמים לינאריים שונים ב-L. הוכיחו כי אם β איבר פרימיטיבי בהרחבה (דהיינו, $L = K(\beta)$) אז גם m_β מתפצל לחלוטין לגורמים לינאריים שונים בתוך L.

תרגיל 13.21 נניח כי $L = K(\alpha_1,\ldots,\alpha_r)$. נסחו והוכיחו טענה מקבילה ללמה 13.14 בעבור הרחבות נוצרות סופית.

13.2.2 חבורת האוטומורפיזמים של הרחבות צקלוטומיות

כעת נחקור את חבורת האוטומורפיזמים של הרחבת שדות פשוטה מסוג מיוחד, הרחבה המכונה צקלוטומית (ושמיד נסביר מה טיבה). יהיו K שדה ו-$\overline{K}$ הסגור האלגברי שלו.

שורש יחידה פרימיטיבי

הגדרה 13.22 יהי $n \geq 2$ מספר טבעי. **שורש יחידה פרימיטיבי מסדר** n בתוך $\overline{K}$ הוא $\zeta \in \overline{K}$ שמקיים $\zeta^n = 1$ אבל $\zeta^m \neq 1$ לכל $1 \leq m < n$.

מעתה נניח כי $n \nmid \operatorname{char} K$, כלומר, $\operatorname{char} K = 0$ או n זר למציין של K. בתרגיל 14.17 להלן נוכיח שתחת ההנחה על המציין של K תמיד קיים שורש פרימיטיבי מסדר n בסגור האלגברי. כאן נניח, ללא הוכחה, שקיים $\zeta \in \overline{K}$ שורש יחידה פרימיטיבי מסדר n, ויהי $L = K(\zeta)$. ההרחבה L/K נקראת **הרחבה צקלוטומית**. על מנת להבין מעט את תכונות חבורת האוטומורפיזמים $\operatorname{Aut}(L/K)$, נזדקק לטענה הבאה:

הרחבה צקלוטומית

טענה 13.23 כל אוטומורפיזם $\sigma \in \operatorname{Aut}(L/K)$ שולח את ζ לאיבר מהצורה ζ^a עם $a \in (\mathbb{Z}/n\mathbb{Z})^*$ (חבורת היחידות של החוג $\mathbb{Z}/n\mathbb{Z}$).

הוכחה: תחילה נטען שגם $\sigma(\zeta)$ הוא שורש יחידה פרימיטיבי מסדר n. אכן, זהו שורש יחידה מסדר n כי

$$(\sigma(\zeta))^n = \sigma(\zeta^n) = \sigma(1) = 1,$$

והוא פרימיטיבי משום שלכל $1 \leq m < n$,

$$(\sigma(\zeta))^m = \sigma(\zeta^m) \neq \sigma(1) = 1.$$

נותר להראות שכל שורש יחידה פרימיטיבי מסדר n הוא מהצורה ζ^a עם $a \in (\mathbb{Z}/n\mathbb{Z})^*$. האיברים $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ כולם שורשי יחידה מסדר n. יתר על כן, כולם שונים זה מזה משום שאם $\zeta^i = \zeta^j$ בעבור $0 \leq i < j \leq n-1$ נקבל $\zeta^{j-i} = 1$ עם $1 \leq j - i \leq n-1$, בסתירה להנחה ש-ζ שורש יחידה פרימיטיבי. מכיוון שלפולינום $x^n - 1 \in K[x]$ יש לכל היותר n שורשים שונים, אלו הם בהכרח בדיוק החזקות השונות הללו של ζ, כלומר, אין שורשי יחידה מסדר n מלבדם. החבורה $\langle\zeta\rangle$ שבתוך L^* היא חבורה צקלית מסדר n, ולכן ζ^a הוא שורש יחידה פרימיטיבי, דהיינו, איבר מסדר n בחבורה $\langle\zeta\rangle$, אם ורק אם $(a, n) = 1$, כלומר, אם ורק אם $a \in (\mathbb{Z}/n\mathbb{Z})^*$ (ראו טענה 1.46). ■

בתנאים הנזכרים לעיל בעבור n, ζ ו-L,

משפטון 13.24 החבורה $\operatorname{Aut}(L/K)$ איזומורפית לתת-חבורה של החבורה $(\mathbb{Z}/n\mathbb{Z})^*$.

הוכחה: תהי

$$\chi : \operatorname{Aut}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^*$$

ההעתקה המוגדרת על ידי $\chi(\sigma) = a$ אם $\sigma(\zeta) = \zeta^a$. נראה כי χ היא שיכון (הומומורפיזם חח״ע) של חבורות: מכיוון ש-$L = K(\zeta)$ היא הרחבה פשוטה של K, כל אוטומורפיזם של ההרחבה נקבע לפי תמונת ζ (למה 13.14), ולכן χ חח״ע. יהיו $\sigma, \tau \in \operatorname{Aut}(L/K)$, ונניח כי $\sigma(\zeta) = \zeta^a$ ו-$\tau(\zeta) = \zeta^b$. אזי

$$(\sigma\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma\left(\zeta^b\right) = (\sigma(\zeta))^b = (\zeta^a)^b = \zeta^{ab},$$

ולכן $\chi(\sigma\tau) = ab = \chi(\sigma) \cdot \chi(\tau)$, כלומר χ הומומורפיזם. אם כן, χ היא שיכון ולכן $\operatorname{Aut}(L/K)$ איזומורפית לתמונתה, שהיא תת-חבורה של $(\mathbb{Z}/n\mathbb{Z})^*$. ■

הערה 13.25 נראה מאוחר יותר (בסעיף 17.2) שבעבור $K=\mathbb{Q}$ השיכון χ הוא **על** ואז $\mathrm{Aut}\left({}^{L}\!/\!{}_{K}\right)$ איזומורפית ל-$(\mathbb{Z}/n\mathbb{Z})^{*}$. אולם, זאת תהא תוצאה בעלת אופי "אריתמטי" וכרגע אנחנו רוצים להתמקד בעובדות הכלליות, בעלות אופי אלגברי.

תרגיל 13.26 הוכיחו כי χ היא על אם ורק אם מעלת הפולינום המינימלי של ζ מעל K היא $\varphi(n)$ (פונקציית אוילר של n — ראו עמוד 21).

תרגיל 13.27 הוכיחו כי ההגדרה של χ בהוכחת משפט 13.24 אינה תלויה ב-ζ. כלומר, אם $\sigma \in \mathrm{Aut}\left({}^{L}\!/\!{}_{K}\right)$ ו-$\chi(\sigma)=a$ אז לכל ρ שורש יחידה פרימיטיבי מסדר n, מתקיים $\sigma(\rho)=\rho^{a}$.

דוגמה 13.28 נתבונן במקרה שבו $K=\mathbb{Q}$ ו-$n=p$ הוא מספר ראשוני. המספר $\zeta=e^{\frac{2\pi i}{p}}\in\mathbb{C}$ הוא שורש יחידה פרימיטיבי מסדר p, ויהי $L=\mathbb{Q}(\zeta)$ שדה ההרחבה שלו מעל $\mathbb{Q}$. בדוגמה 11.19 ראינו כי הפולינום המינימלי של ζ מעל $\mathbb{Q}$ הוא

$$m_{\zeta}=x^{p-1}+x^{p-2}+\ldots+x+1\ ,$$

(נעזרנו בקריטריון אייזנשטיין על מנת להוכיח שפולינום זה אי-פריק), ולפיכך $[L:\mathbb{Q}]=\deg m_{\zeta}=p-1$. כל p החזקות השונות $1,\zeta,\zeta^{2},\ldots,\zeta^{p-1}$ הן שורשי יחידה מסדר p ולכן שורשים של $x^{p}-1=(x-1)\cdot m_{\zeta}$, אך רק 1 הוא שורש של הגורם $(x-1)$. לכן כל $p-1$ החזקות $\zeta,\zeta^{2},\ldots,\zeta^{p-1}$ הן שורשים של m_{ζ}, שכמובן שייכות ל-$L=\mathbb{Q}(\zeta)$. מלמה 13.15 נסיק שלכל $1\leq a\leq p-1$ יש אוטומורפיזם $\sigma\in\mathrm{Aut}\left({}^{L}\!/\!{}_{\mathbb{Q}}\right)$ ששולח את ζ ל-ζ^{a}. במקרה זה, אם כן, ההעתקה χ מהוכחת משפט 13.24 היא על, ולכן

$$\mathrm{Aut}\left({}^{L}\!/\!{}_{\mathbb{Q}}\right)\cong(\mathbb{Z}/p\mathbb{Z})^{*}=\mathbb{F}_{p}^{*}.$$

למעשה, מכיוון שהחבורה הכפלית של שדה סופי היא צקלית (משפט 11.49), החבורה הכפלית של $\mathbb{F}_{p}^{*}$ היא צקלית מסדר $p-1$, ולכן $\mathrm{Aut}\left({}^{L}\!/\!{}_{\mathbb{Q}}\right)$ איזומורפית גם לחבורה הצקלית $\mathbb{Z}_{p-1}$.

תרגיל 13.29 לכל $n\geq 2$, מצאו את $\mathrm{Aut}\left({}^{\mathbb{R}(\zeta)}\!/\!{}_{\mathbb{R}}\right)$ ואת תת-החבורה המתאימה לה בתוך $(\mathbb{Z}/n\mathbb{Z})^{*}$ כאשר ζ הוא שורש יחידה פרימיטיבי מסדר n מעל $\mathbb{R}$.

13.3 שדה פיצול של פולינום

יהי K שדה ו-$f\in K[x]$ פולינום כלשהו. ראינו כבר כי יש שדות הרחבה של K שבהם יש ל-f שורש, ואף שיש שדות הרחבה שבהם f מתפצל, כלומר, מתפרק לחלוטין לגורמים לינאריים: למשל, הסגור האלגברי של K. כמובן, על-פי רוב ישנם גם שדות קטנים יותר שבהם f מתפצל. חשיבות מיוחדת נתונה לשדות הרחבה שכאלה שהם מינימליים ביחס להכלה:

שדה פיצול

הגדרה 13.30 יהי $f\in K[x]$. שדה הרחבה ${}^{L}\!/\!{}_{K}$ ייקרא **שדה פיצול** (splitting field) של f אם
1. f מתפצל ב-L.
2. L מינימלי עם תכונה זו, ביחס להכלת שדות. כלומר, אם $K\subseteq L'\subseteq L$ ו-f מתפצל כבר מעל L', אז $L'=L$.

לעתים המונח "שדה פיצול" משמש לשדות הרחבה שמקיימים את תכונה (1) בלבד, אך אנו נדבוק בהגדרה המצומצמת יותר. שימו לב, בנוסף, כי אם f מתפצל מעל שדה הרחבה כלשהו M של K ושורשיו ב-M

הם $\alpha_1, \ldots, \alpha_r$, אז $K(\alpha_1, \ldots, \alpha_r)$ הוא שדה פיצול של f. כלומר, L הוא שדה פיצול של f מעל K אם ורק אם f מתפצל בו ו-L נוצר על-ידי שורשיו של f.

בסעיף 15.3 נכיר תכונות נוספות של שדה הפיצול. כעת, ברצוננו להתמקד בתכונות חבורת האוטומורפיזמים $\mathrm{Aut}(L/K)$ כאשר L הוא שדה פיצול של $f \in K[x]$. נזכיר כי אם X קבוצה, אנו מסמנים ב-S_X את חבורת התמורות של X (ראו סעיף 1.1.1 או פרק 4).

משפט 13.31 יהיו K שדה, $f \in K[x]$ פולינום ו-L שדה פיצול של f. יהיו $\alpha_1, \ldots, \alpha_r$ שורשי f ב-L. אזי,

1. קיים שיכון, כלומר, הומומורפיזם חח״ע, לתוך חבורת התמורות $\mathrm{Aut}(L/K) \hookrightarrow S_{\{\alpha_1, \ldots, \alpha_r\}} \cong S_r$.
2. $|\mathrm{Aut}(L/K)|$ מחלק את $r!$.

הוכחה: ראשית, נזכיר כי חבורת התמורות על קבוצה בגודל r איזומורפית ל-S_r, ולכן $S_{\{\alpha_1, \ldots, \alpha_r\}} \cong S_r$. יהי $\sigma \in \mathrm{Aut}(L/K)$ אוטומורפיזם. מכיוון ש-$f \in K[x]$, מקדמיו מקובעים על-ידי σ, ולכן אם α_i שורש של f, גם $\sigma(\alpha_i)$ שורש של f. מאידך, σ הוא חח״ע. לפיכך, הצמצום $\sigma|_{\{\alpha_1, \ldots, \alpha_r\}}$ הוא תמורה. לכן ניתן להגדיר העתקה $\psi : \mathrm{Aut}(L/K) \to S_{\{\alpha_1, \ldots, \alpha_r\}}$ על-ידי

$$\sigma \mapsto \sigma|_{\{\alpha_1, \ldots, \alpha_r\}}.$$

נראה כי ψ היא שיכון: הואיל ו-L שדה פיצול של f מעל K, מתקיים $L = K(\alpha_1, \ldots, \alpha_r)$. לפי תרגיל 13.21, שמכליל את למה 13.14, כל אוטומורפיזם $\sigma \in \mathrm{Aut}(L/K)$ נקבע לפי פעולתו על קבוצת יוצרים של L מעל K, כלומר, נקבע לפי פעולתו על $\alpha_1, \ldots, \alpha_r$. במלים אחרות, אם σ_1 ו-σ_2 מזדהים בפעולתם על $\alpha_1, \ldots, \alpha_r$, אזי הם אותו אוטומורפיזם. לפיכך ההעתקה ψ היא חח״ע. היא הומומורפיזם משום שלכל $\sigma_1, \sigma_2 \in \mathrm{Aut}(L/K)$ ברור כי $(\sigma_1\sigma_2)|_{\{\alpha_1, \ldots, \alpha_r\}} = \left(\sigma_1|_{\{\alpha_1, \ldots, \alpha_r\}}\right)\left(\sigma_2|_{\{\alpha_1, \ldots, \alpha_r\}}\right)$. בכך הוכחנו את הטענה הראשונה של המשפט.

הטענה השניה נובעת מהטענה הראשונה ביחד עם משפט לגרנז׳ (משפט 1.81), שכן ראינו ש-$\mathrm{Aut}(L/K)$ איזומורפית לתת-חבורה S_r, והסדר של S_r הוא $r!$. ■

דוגמה 13.32 תהי $L = K(\zeta)$ הרחבה צקלוטומית כאשר ζ שורש יחידה פרימיטיבי מסדר n. בפרט, L היא שדה הפיצול מעל K של הפולינום $x^n - 1$ (מדוע?). לפיכך, $\mathrm{Aut}(L/K)$ איזומורפית לתת-חבורה של

$$S_{\{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}} \cong S_n.$$

אולם במקרה זה יש פער גדול בין $\mathrm{Aut}(L/K)$ לכל S_n. ראשית, את השורש 1 כל אוטומורפיזם חייב לקבע (להותיר במקום). שנית, תמונת השורש ζ דרך σ קובעת את התמונות של כל יתר השורשים כי הם כולם חזקות של ζ (כלומר, $\sigma(\zeta^i) = (\sigma(\zeta))^i$). לכן יש לנו מעט מאוד חופש בבחירת תמורה על השורשים שמתאימה לאוטומורפיזם. למעשה, כפי שראינו בסעיף הקודם, $\mathrm{Aut}(L/K)$ איזומורפית, במקרה זה, לתת-חבורה של $(\mathbb{Z}/n\mathbb{Z})^*$, ועל כן גודלה לכל היותר $\varphi(n)$, שהוא נמוך אף מ-n (ולא רק מ-$n!$).

דוגמה 13.33 בהמשך לדוגמה 13.18, יהי הפעם השדה L הרחבה של $\mathbb{Q}$ בתוך $\mathbb{C}$ שהיא שדה הפיצול של $x^3 - 2 \in \mathbb{Q}[x]$. מכיוון ששורשי פולינום זה ב-$\mathbb{C}$ הם α, $\alpha\omega$ ו-$\alpha\omega^2$, כאשר $\alpha = \sqrt[3]{2}$ הוא השורש הממשי ו-$\omega = e^{\frac{2\pi i}{3}}$, נקבל כי $L = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$. קל לראות כי $L = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2) = \mathbb{Q}(\alpha, \omega)$ (מדוע?). ציינו כבר כי $\mathbb{Q}(\alpha)$ מוכל ב-$\mathbb{R}$ ולכן $\mathbb{Q}(\alpha) \subsetneqq L$. מצד שני, $\omega^2 + \omega + 1 = \frac{\omega^3 - 1}{\omega - 1} = 0$, כלומר ω מאפס את הפולינום $x^2 + x + 1 \in \mathbb{Q}(\alpha)[x]$, ולכן דרגת ההרחבה $[L : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(\omega) : \mathbb{Q}(\alpha)] \leq 2$.

לפיכך $[L:\mathbb{Q}(\alpha)]=2$, ו-

$$[L:\mathbb{Q}]=[L:\mathbb{Q}(\alpha)]\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]=2\cdot 3=6\ .$$

ננסה להבין כעת את מבנה החבורה $\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)$. יהי אם כן $\sigma\in\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)$. לפי משפט 13.31, σ מתאים לתמורה על $\{\alpha,\alpha\omega,\alpha\omega^2\}$, קבוצת השורשים של x^3-2 ו-$\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)$ איזומורפית לתת-חבורה של S_3. למעשה, במקרה זה ניתן להראות כי כל התמורות על $\{\alpha,\alpha\omega,\alpha\omega^2\}$ מגדירות אוטומורפיזמים "כשרים", וכי, למעשה, $\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)\cong S_3$ (נראה זאת בתרגיל שלהלן).

תרגיל 13.34 הוכיחו כי בדוגמה האחרונה אמנם $\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)\cong S_3$. הדרכה:

1. הוכיחו כי אוטומורפיזם ההצמדה $\tau\in\mathrm{Aut}\left({}^{\mathbb{C}}\!/\!_{\mathbb{R}}\right)$ מצטמצם לאוטומורפיזם של L שמקבע את $\mathbb{Q}$, כלומר $\tau|_L\in\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)$.
2. לאיזו תמורה ב-$S_{\{\alpha,\alpha\omega,\alpha\omega^2\}}$ מתאים $\tau|_{\mathrm{L}}$?
3. הוכיחו כי $[L:\mathbb{Q}(\omega)]=3$ והסיקו כי x^3-2 הוא הפולינום המינימלי של α גם מעל $\mathbb{Q}(\omega)$.
4. בעזרת הסעיף הקודם ולמה 13.15, הראו שיש $\sigma\in\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)$ ששולח את α ל-$\alpha\omega$ ומקבע את ω. לאיזו תמורה ב-$S_{\{\alpha,\alpha\omega,\alpha\omega^2\}}$ הוא מתאים?
5. הסיקו כי $\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)\cong S_{\{\alpha,\alpha\omega,\alpha\omega^2\}}\cong S_3$.

13.4 התאמת גלואה

תהי ${}^{L}\!/\!_{K}$ הרחבת שדות. ההתאמה הבאה, שניסח גלואה, מתאימה לכל תת-חבורה של $\mathrm{Aut}\left({}^{L}\!/\!_{K}\right)$ שדה ביניים שנמצא "בין K ל-L", כלומר מכיל את K ומוכל ב-L, ומתאימה לכל שדה ביניים כזה תת-חבורה של $\mathrm{Aut}\left({}^{L}\!/\!_{K}\right)$:

$\boxed{\mathcal{G}(M)}$ $\boxed{\mathcal{F}(H)}$

הגדרה 13.35 תהי ${}^{L}\!/\!_{K}$ הרחבת שדות ותהי $G=\mathrm{Aut}\left({}^{L}\!/\!_{K}\right)$. לכל שדה ביניים $K\subseteq M\subseteq L$, התאמה גלואה מתאימה את החבורה $\mathcal{G}(M)=\mathrm{Aut}\left({}^{L}\!/\!_{M}\right)$, ולכל תת-חבורה $H\leq G=\mathrm{Aut}\left({}^{L}\!/\!_{K}\right)$ מתאימה את **שדה השבת** של H המסומן $\mathcal{F}(H)$ ומוגדר על-ידי

$$\mathcal{F}(H)=\{x\in L\mid \sigma(x)=x \text{ לכל } \sigma\in H\}.$$

אם כן, $\mathcal{F}$ ו-$\mathcal{G}$ הן פונקציות בין קבוצה שדות הביניים לקבוצת תת-החבורות

$$\{M\mid K\subseteq M\subseteq L\}\qquad\qquad \{H\mid H\leq\mathrm{Aut}\left({}^{L}\!/\!_{K}\right)\}$$

המוגדרות כ-

$$\begin{array}{ccc} M & \longmapsto & \mathcal{G}(M)=\mathrm{Aut}\left({}^{L}\!/\!_{M}\right) \\ \text{שדה השבת}=\mathcal{F}(H) & \longleftarrow\!\shortmid & H \end{array},$$

כאשר שדה השבת $\mathcal{F}(H)$ הוא קבוצת האיברים ב-L שמקובעים על-ידי כל האוטומורפיזמים ב-H.

טענה 13.36

1. $\mathcal{F}(H)$ הוא אמנם שדה, ואף שדה ביניים: $K\subseteq\mathcal{F}(H)\subseteq L$.
2. $\mathcal{F}(\{e\})=L$.
3. אם $H_1\leq H_2$ אז $\mathcal{F}(H_1)\supseteq\mathcal{F}(H_2)$.

הוכחה: (1) ברור כי $\mathcal{F}\left(H\right)$ זו תת-קבוצה של L שמכילה את K, לפי ההגדרות של $\mathcal{F}\left(H\right)$ ושל $G=\operatorname{Aut}\left(L/K\right)$. בנוסף, אם $\sigma\left(x\right)=x$ ו-$\sigma\left(y\right)=y$ אז $\sigma\left(x\pm y\right)=x\pm y$, $\sigma\left(xy\right)=xy$ וכן $\sigma\left(x^{-1}\right)=x^{-1}$, ולפיכך $\mathcal{F}\left(H\right)$ הוא תת-שדה של L.

(2) הטענה מובנת מאליה.

(3) במעבר מ-H_1 ל-H_2 רק הרחבנו את מעגל האילוצים על האיברים של $\mathcal{F}\left(H_2\right)$, ולכן ברור שמתקיימת ההכלה $\mathcal{F}\left(H_1\right)\supseteq\mathcal{F}\left(H_2\right)$. ∎

שימו לב שבהוכחת סעיף (1) של הטענה כלל לא השתמשנו בכך ש-H היא תת-חבורה. למעשה, באופן כללי יותר, לכל תת-קבוצה $S\subseteq\operatorname{Aut}\left(L\right)$, הקבוצה $\mathcal{F}\left(S\right)$ היא תת-שדה של L.

טענה 13.37

1. $\mathcal{G}\left(M\right)$ היא תת-חבורה: $\mathcal{G}\left(M\right)\leq G$.
2. $\mathcal{G}\left(L\right)=\{e\}$ ו-$\mathcal{G}\left(K\right)=G$.
3. אם $M_1\subseteq M_2$ אז $\mathcal{G}\left(M_1\right)\geq\mathcal{G}\left(M_2\right)$.

תרגיל 13.38 הוכיחו את טענה 13.37.

נזכיר כי החבורה $\mathcal{G}\left(M\right)$ היא חבורת האוטומורפיזמים $\operatorname{Aut}\left(L/M\right)$. עם זאת, שימו לב שגם במקרה זה, סעיף (1) של טענה 13.37 נכון גם ללא ההנחה ש-M הוא שדה ביניים: די להניח כי הוא תת-קבוצה של L שמכילה את K.

הערה 13.39 שימו לב שטענות 13.36 ו-13.37 סימטריות, לבד מנקודה אחת: בסעיף (2) של הראשונה לא טענו כי $K=\mathcal{F}\left(G\right)$. בהמשך נראה כי תכונה זו אינה מתקיימת תמיד. למעשה, קיומה שקול להיותה של ההרחבה L/K "הרחבת גלואה", מושג שנגדיר מיד (ראו מסקנה 16.2).

טענה 13.40 לכל שדה ביניים M מתקיים $M\subseteq\mathcal{F}\left(\mathcal{G}\left(M\right)\right)$.
לכל תת-חבורה H מתקיים $H\leq\mathcal{G}\left(\mathcal{F}\left(H\right)\right)$.

הוכחה: הטענה נובעת ישירות מההגדרות: כל איבר של M מקובע על-ידי כל אוטומורפיזם שמקבע את כל איברי M. כל אוטומורפיזם ב-H מקבע נקודתית את כל איברי השדה שמקובעים נקודתית על-ידי כל איברי H. ∎

תרגיל 13.41 הוכיחו כי $\mathcal{G}\left(\mathcal{F}\left(\mathcal{G}\left(M\right)\right)\right)=\mathcal{G}\left(M\right)$ וכן $\mathcal{F}\left(\mathcal{G}\left(\mathcal{F}\left(H\right)\right)\right)=\mathcal{F}\left(H\right)$.
במלים אחרות, אחרי איטרציה אחת ההכלה מטענה 13.40 הופכת לשוויון.

דוגמאות

דוגמה 13.42 בדוגמה 13.12 ראינו כי $G=\operatorname{Aut}\left(\mathbb{C}/\mathbb{R}\right)=\{e,\tau\}$, כאשר τ הוא אוטומורפיזם ההצמדה. משיקולי דרגות הרחבה, למשל, אין שדות ביניים (פרט ל-$\mathbb{R}$ ול-$\mathbb{C}$ עצמם). כמובן, אין גם תת-חבורות ממש ל-G. התאמת גלואה שולחת את G ל-$\mathbb{R}$ ‏$\mathcal{F}\left(G\right)=\mathbb{R}$ ואת $\mathbb{R}$ בחזרה ל-G ‏$\mathcal{G}\left(\mathbb{R}\right)=G$. היא מתאימה גם את החבורה $\{e\}$ ואת השדה $\mathbb{C}$ זה לזה.

דוגמה 13.43 בדוגמה 13.18 התבוננו בהרחבה של $\mathbb{Q}$ על-ידי $\alpha=\sqrt[3]{2}\in\mathbb{C}$. ראינו כי $\operatorname{Aut}\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right)=\{e\}$. אין כאן שדות ביניים לא טריוויאליים (מדוע?), ומתקיים

$$\mathcal{G}\left(\mathbb{Q}\right)=\mathcal{G}\left(\mathbb{Q}\left(\alpha\right)\right)=\{e\}$$

ואילו $\mathcal{F}(\{e\}) = \mathbb{Q}(\alpha)$.

דוגמה 13.44 נתבונן בשדה $L = \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$. כדי להבין מה טיב ההרחבה ${}^{L}\!/\!_{\mathbb{Q}}$ נראה תחילה כי $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$. אכן, הפולינום המינימלי של $\sqrt{2}$ מעל $\mathbb{Q}$ הוא x^2-2. לפי מסקנה 11.21 והפסקה שלאחריה, $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a+b\sqrt{2} \,\middle|\, a,b \in \mathbb{Q}\right\}$. נניח בשלילה כי $\sqrt{3} = a+b\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$. אם נעלה בריבוע את שני האגפים נקבל

$$3 = a^2 + 2ab\sqrt{2} + 2b^2,$$

ולכן $\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$, בסתירה לעובדה הידועה ש-$\sqrt{2}$ אינו רציונלי[7]. (לשם הדיוק, עלינו לוודא גם שלא ייתכן כי $ab=0$. ודאו זאת.)

מכיוון ש-$\sqrt{3}$ מאפס את הפולינום x^2-3 מעל $\mathbb{Q}\left(\sqrt{2}\right)$, מתקיים $\left[\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$, ולכן

$$[L:\mathbb{Q}] = \left[L:\mathbb{Q}\left(\sqrt{2}\right)\right]\cdot\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right] = 2\cdot 2 = 4.$$

מכאן ניתן להסיק כי $\sqrt{2} \notin \mathbb{Q}\left(\sqrt{3}\right)$, שהרי $\left[\mathbb{Q}\left(\sqrt{3}\right):\mathbb{Q}\right] = 2$ ולכן $\mathbb{Q}\left(\sqrt{3}\right) \subsetneqq \mathbb{Q}\left(\sqrt{3},\sqrt{2}\right)$. מצאנו אפוא שני שדות ביניים, כפי שמתואר בשרטוט הבא:

$$\begin{tikzcd}[column sep=small]
 & L = \mathbb{Q}\left(\sqrt{2},\sqrt{3}\right) \arrow[dl, dash] \arrow[dr, dash] & \\
E = \mathbb{Q}\left(\sqrt{2}\right) \arrow[dr, dash] & & F = \mathbb{Q}\left(\sqrt{3}\right) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

לפי תרגיל 13.21, כל $\sigma \in \mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)$ נקבע לפי פעולתו על היוצרים $\sqrt{2}$ ו-$\sqrt{3}$. אך, כרגיל, $\sigma\left(\sqrt{2}\right)$ הוא שורש של הפולינום x^2-2 ולכן $\sigma\left(\sqrt{2}\right) \in \left\{\sqrt{2},-\sqrt{2}\right\}$. באופן דומה, $\sigma\left(\sqrt{3}\right) \in \left\{\sqrt{3},-\sqrt{3}\right\}$, ועל כן יש לכל היותר ארבעה אוטומורפיזמים במקרה זה. האם כל ארבע האפשרויות מגדירות אוטומורפיזם "כשר"?

כדי לענות על שאלה זאת, ננסה תחילה להבין מהן חבורות האוטומורפיזמים המתאימות לשדות הביניים E ו-F. החבורה המתאימה ל-E היא $\mathcal{G}(E) = \mathrm{Aut}\left({}^{L}\!/\!_{E}\right) \le \mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)$. מכיוון ש-$L = E\left(\sqrt{3}\right)$, זו הרחבה ריבועית פשוטה. לפי למה 13.15, יש בה אוטומורפיזם לכל שורש של x^2-3 שנמצא בתוך L. אבל שני השורשים שייכים ל-L ולכן, לצד אוטומורפיזם הזהות, יש גם אוטומורפיזם σ ששולח את $\sqrt{3}$ ל-$-\sqrt{3}$. מכיוון ש-$\sigma \in \mathrm{Aut}\left({}^{L}\!/\!_{E}\right)$, הוא מקבע את איברי E, ובפרט את $\sqrt{2}$.

באופן דומה, $\mathcal{G}(F) = \mathrm{Aut}\left({}^{L}\!/\!_{F}\right) = \{e,\tau\}$ כאשר $\tau\left(\sqrt{2}\right) = -\sqrt{2}$ ואילו $\tau\left(\sqrt{3}\right) = \sqrt{3}$. מצאנו כבר שלושה אוטומורפיזמים ב-$\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right)$: e, σ ו-τ. נסמן $\theta = \tau\cdot\sigma$ ונשים לב כי

$$\theta\left(\sqrt{2}\right) = \tau\left(\sigma\left(\sqrt{2}\right)\right) = \tau\left(\sqrt{2}\right) = -\sqrt{2}$$
$$\theta\left(\sqrt{3}\right) = \tau\left(\sigma\left(\sqrt{3}\right)\right) = \tau\left(-\sqrt{3}\right) = -\sqrt{3}$$

ולכן θ שונה מ-σ ומ-τ. קיבלנו כי $\mathrm{Aut}\left({}^{L}\!/\!_{\mathbb{Q}}\right) = \{e,\sigma,\tau,\theta\}$ (זכרו כי עוד קודם ראינו כי יש בחבורה זו לכל היותר ארבעה איברים). מכיוון שכל האוטומורפיזמים פרט ל-e הם מסדר 2, חבורה זו איזומורפית

[7] מומלץ למי שאינו מכיר את ההוכחה הפשוטה של עובדה זו לנסות לגלותה בעצמו או לחפשה במרשתת (האינטרנט).

ל-$\mathbb{Z}_2 \times \mathbb{Z}_2$ (ולא לחבורה האחרת מסדר 4, הלוא היא $\mathbb{Z}_4$).
על-מנת להבין מהם שדות השבת המתאימים לתת-החבורות של $\mathrm{Aut}\left({}^{L}\!/\!{}_{\mathbb{Q}}\right)$, נמצא קודם בסיס ל-$L$ מעל $\mathbb{Q}$ ונכתוב באמצעותו את איברי L. לפי הוכחת משפט 11.9, די למצוא בסיס ל-${}^{\mathbb{Q}(\sqrt{2})}\!/\!{}_{\mathbb{Q}}$ ול-${}^{L}\!/\!{}_{\mathbb{Q}(\sqrt{2})}$. קל לראות כי $\left\{1, \sqrt{2}\right\}$ הוא בסיס להרחבה הראשונה ו-$\left\{1, \sqrt{3}\right\}$ בסיס להרחבה השניה, ומהוכחת משפט 11.9 נובע כי $\left\{1, \sqrt{2}\right\} \cdot \left\{1, \sqrt{3}\right\} = \left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$ בסיס ל-${}^{L}\!/\!{}_{\mathbb{Q}}$. לכן

$$L = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \;\middle|\; a, b, c, d \in \mathbb{Q}\right\}.$$

כעת נוכל למצוא בייתר קלות את שדות השבת המתאימים לתת-החבורות השונות. למשל, בעבור $H = \{e, \theta\} \leq \mathrm{Aut}\left({}^{L}\!/\!{}_{\mathbb{Q}}\right)$, שדה השבת מורכב מאיברי L שמקובעים על-ידי θ (כולם מקובעים, כמובן, על-ידי e). מכיוון ש-

$$\theta\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6},$$

נקבל כי $\mathcal{F}(H) = \left\{a + d\sqrt{6} \;\middle|\; a, d \in \mathbb{Q}\right\}$. שדה זה אינו אלא $\mathbb{Q}\left(\sqrt{6}\right)$, שהוא שדה ביניים נוסף על השניים שלעיל. באופן דומה, $E = \mathcal{F}(\langle\sigma\rangle)$ ו-$F = \mathcal{F}(\langle\tau\rangle)$. נסכם דוגמה זו בשרטוט הבא שמציב אלה אל מול אלה את שדות הביניים שמצאנו בהרחבה ${}^{L}\!/\!{}_{\mathbb{Q}}$ ואת תת-החבורות של $\mathrm{Aut}\left({}^{L}\!/\!{}_{\mathbb{Q}}\right)$. שימו לב שבדוגמה זו ההתאמה מכיוון אחד היא בדיוק ההפכית להתאמה מן הכיוון השני.

$$\begin{tikzcd}[column sep=small]
 & L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
E = \mathbb{Q}\left(\sqrt{2}\right) \arrow[dr, dash] & K = \mathbb{Q}\left(\sqrt{6}\right) \arrow[d, dash] & F = \mathbb{Q}\left(\sqrt{3}\right) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \{e\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{e, \sigma\} \arrow[dr, dash] & \{e, \theta\} \arrow[d, dash] & \{e, \tau\} \arrow[dl, dash] \\
 & \mathrm{Aut}\left({}^{L}\!/\!{}_{\mathbb{Q}}\right) &
\end{tikzcd}$$

(שימו לב שאנו מציגים כאן ובדוגמאות שלהלן את שריג תת-החבורות "הפוך": ככל שחבורה גדולה יותר, כך היא תמצא במקום נמוך יותר בשרטוט.)

תרגיל 13.45 השלימו את פרטי הדוגמה האחרונה:

1. ודאו כי אמנם כל תת-חבורה ושדה ביניים שמצויים באותו מיקום בשני השריגים מתאימים זה לזה לפי התאמת גלואה.
2. רשמו את פעולת τ ו-σ על איברי L שרשומים כצירופים לינאריים של איברי הבסיס שמצאנו.
3. הוכיחו כי במקרה זה אין שדות ביניים נוספים לאלו שמצאנו.

רמז: ניתן להיעזר בתרגיל 11.12.

דוגמה 13.46 בדוגמה 13.28 ראינו כי $G = \mathrm{Aut}\left({}^{\mathbb{Q}(\zeta)}\!/\!{}_{\mathbb{Q}}\right) \cong \mathbb{Z}_p^*$, כאשר $\zeta = e^{\frac{2\pi i}{p}}$ ו-p ראשוני. כדוגמה, נביט במקרה $p = 5$, אז החבורה היא $G \cong \mathbb{Z}_5^*$ שאיזומורפית גם לחבורה הצקלית מסדר 4. יהי σ האוטומורפיזם ששולח את ζ ל-ζ^2, וקל לבדוק כי $G = \langle\sigma\rangle$ (כי $\langle 2\rangle = \mathbb{Z}_5^*$). ל-$G$ יש בדיוק שלוש תת-

חבורות: $\{e\}$, $\{e,\sigma\}$ ו-G. התאמת גלואה במקרה זה תיתן את שדות הביניים הבאים:

$$\begin{array}{ccc} \mathbb{Q}(\zeta) & & \{e\} \\ | & & | \\ \mathbb{Q}\left(\zeta+\zeta^{-1}\right)=\mathbb{Q}\left(\cos\frac{2\pi}{5}\right) & & \{e,\sigma_4\} \\ | & & | \\ \mathbb{Q} & & G \end{array}$$

תרגיל 13.47 השלימו את הפרטים בדוגמה האחרונה: הראו כי אכן אלו שדות השבת המתאימים לתת-חבורות השונות. מצאו את דרגות ההרחבה של השדות, והראו כי גם במקרה זה התאמת גלואה היא חח״ע ועל, כלומר ההתאמה מהשדות לחבורות הפכית להתאמה מהחבורות לשדות.

דוגמה 13.48 בדוגמה 13.19 ראינו כי בעבור $K=\mathbb{F}_p(t)$, $\alpha=\sqrt[p]{t}$ ו-$L=K(\alpha)$, החבורה $\mathrm{Aut}\left({}^{L}/_{K}\right)$ היא טריוויאלית. מכיוון ש-$[L:K]=p$ אין שדות ביניים בין K ל-L פרט להם עצמם (הרי לפי כפליות דרגות ההרחבה, כל שדה ביניים ממש היה נותן פירוק של הראשוני p, בסתירה). אולם, ההתאמה ששולחת שדות-ביניים לחבורות איננה חח״ע: מתקיים $\mathcal{G}(L)=\mathcal{G}(K)=\{e\}$.

הרחבת גלואה

בפרקים הקרובים, המטרה שלנו תהיה למצוא תנאים שבהם $\mathcal{F}$ ו-$\mathcal{G}$ הן התאמות הפכיות בין שריגים של חבורות ביניים ושל שדות ביניים. נראה כי הרחבה סופית ${}^{L}/_{K}$ צריכה לקיים לשם כך שני תנאים — **נורמליות** ו**ספרביליות**.

נורמליות פרושה ״אם שורש אחד בהרחבה, כל השורשים בהרחבה״: אם לפולינום אי-פריק מעל $K[x]$ יש שורש בהרחבה L, אז כל שורשיו ב-L, כלומר, הוא מתפצל לחלוטין, לגורמים לינאריים, בתוך $L[x]$. למשל, בדוגמה 13.18 לפולינום האי-פריק $x^3-2\in\mathbb{Q}[x]$ יש שורש בהרחבה $\mathbb{Q}(\alpha)$, אך שני השורשים האחרים שלו אינם בהרחבה זו. לפיכך ${}^{\mathbb{Q}(\alpha)}/_{\mathbb{Q}}$ אינה נורמלית. על מושג הנורמליות בהרחבות של שדות נלמד בפירוט רב יותר בפרק 15.

ספרביליות (או **פרידות**), פירושה שאין שורשים כפולים: כל פולינום אי-פריק מעל K מתפרק ב-$L[x]$ לגורמים אי-פריקים **שונים**. ההרחבה בדוגמה 13.19 אינה ספרבילית: הפולינום האי-פריק $x^p-t\in K[x]$ מתפרק בתוך $L[x]$ ל-$(x-\alpha)^p$. את מושג הספרביליות נפתח עוד בפרק 14.

הרחבת גלואה סופית

הרחבת שדות סופית ${}^{L}/_{K}$ תקרא **הרחבת גלואה** אם היא נורמלית וספרבילית. נראה בהמשך (בפרק 16) שבמקרה זה אמנם ההתאמות $\mathcal{F}$ ו-$\mathcal{G}$ הפכיות זו לזו. יתר על כן, נראה כי תנאי שקול לכך הוא ש-${}^{L}/_{K}$ שדה פיצול של פולינום שכל שורשיו שונים זה מזה. ניתן גם תנאי נומרי שקול ונוכיח ש-${}^{L}/_{K}$ גלואה אם ורק אם $\left|\mathrm{Aut}\left({}^{L}/_{K}\right)\right|=[L:K]$ ושאחרת תמיד קיים אי-שוויון $\left|\mathrm{Aut}\left({}^{L}/_{K}\right)\right|<[L:K]$.

לדוגמה, ההרחבה ${}^{\mathbb{Q}\left(\sqrt[3]{2}\right)}/_{\mathbb{Q}}$ איננה הרחבת גלואה משום שכאמור, היא איננה נורמלית, ואכן, חבורת האוטומורפיזמים בגודל 1 בעוד שההרחבה מדרגה 3. ההרחבה $K=\mathbb{F}_p(t)\subseteq L=\mathbb{F}_p\left(\sqrt[p]{t}\right)$ שבדוגמה 13.19 איננה הרחבת גלואה משום שהיא איננה ספרבילית: הפולינום האי-פריק $x^p-t\in K[x]$ מתפרק ל-$(x-\alpha)^p$ בתוך $L[x]$. גם שם, חבורת האוטומורפיזמים טריוויאלית בעוד שההרחבה מממד p.
לעומת זאת, בדוגמה $\mathbb{Q}\subseteq L=\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$, ההרחבה היא נורמלית וספרבילית (בפרקים הבאים נפתח כלים להוכיח זאת) ועל-כן גלואה. כפי שראינו, ההתאמות $\mathcal{F}$ ו-$\mathcal{G}$ אמנם הפכיות זו לזו במקרה זה,

וכן

$$|\mathrm{Aut}\left({}^{L}/_{\mathbb{Q}}\right)| = 4 = [L : \mathbb{Q}] \, .$$

מצב דומה מתקיים גם בדוגמה $\mathbb{Q} \subseteq \mathbb{Q}\left(e^{2\pi i/5}\right)$ שניתחנו בסעיף הקודם.

תרגיל 13.49 בדוגמה 13.33 ובתרגיל 13.34 שלאחריה, חקרנו את שדה הפיצול L של $x^3 - 2$ מעל $\mathbb{Q}$ (בתוך $\mathbb{C}$).

1. מצאו את כל תת-החבורות של $\mathrm{Aut}\left({}^{L}/_{\mathbb{Q}}\right)$, ומצאו את שדה השבת המתאים לכל אחת מהן.
2. מצאו את החבורה המתאימה לכל אחד משדות השבת שמצאתם.
3. בהנחה שאין שדות ביניים נוספים, האם ההתאמות $\mathcal{F}$ ו-$\mathcal{G}$ הפכיות בדוגמה זו?