אחת מהנקודות בקו המחבר בין האלגברה הקלאסית שעניינה פתרון משוואות, לאלגברה המודרנית, שעניינה חקר של מבנים אלגברים, היא ההתאמה שבסיסה של תורת גלואה, המציגה את הקשר בין הרחבות של שדות לחבורות האוטומורפיזמים שהם משרים.

על סיפור חייו הרומנטיים כבר נכתב רבות; אך לדעתי, מעניינת כמוהו היא ההבנה של התרומה המתמטית שהעמיד. שכן לא רק שמאמרו המקורי נדחה שוב ושוב בימי חייו, אלא שגם לא עמדו לרשותו חלק מהכלים שאנו משתמשים בהם היום כדי לתאר את מסקנותיו—שכן המונחים לתיאור של שדות והרחבותיהם ניתנו בראשונה ע"י דדיקנד ב-1894, בהשפעה ישירה של גלואה.

עבודה זו מנסה לתת קריאה מודרנית של המאמר "*Memoir sur les conditions de résolubilité des équations par radicaux*"—שפורסם במקור ע"י ליוביל, ב-1846, 14 שנים לאחר מותו של גלואה—ולתאר את הטקטיקה שבה הוא בוחר להגיע לתוצאה העיקרית שלו, דהיינו ההתאמה בין שדות הביניים של הרחבה לחבורות האוטומורפיזמים המשאירות אותם במקום, מול זו שמשתמשים בה כיום.

בהצגת הניסוח המודרני אני עוקב אחרי סיכומי ההרצאות של ארטין, שהיה הראשון לנסח אותו בצורה המלאה המוכרת לנו כיום.

קודמיו של גלואה

את היסודות לעבודתו של גלואה ניתן למצוא במאמר של לגרנג' מ-1770-1771, "*Réflexions sur la résolution algebrique des équations*". לעומת קודמיו, שניסו למצוא את הטריק החישובי שיאפשר פתרון פולינומים ממעלה חמישית, לגרנג' ניגש לבעיה *a priori*: הוא חוקר את השיטות לפתרון פולינומים שהיו ידועות עד אז, כדי להבין לא רק איך, אלא גם מדוע הן עובדות, וכיצד ניתן יהיה להרחיב אותן לבעיה הכללית של פתרון פולינום כלשהו.

אף על פי שהמטרה שעומדת לנגד עינייו היא עדיין חישובית גרידא, הוא עובד בדרך אבסטרקטית יותר מהמקובל עד אז: ראשית, הוא מחדש ונותן סימנים לשורשי הפולינום, ומשתמש בהם בחישוביו כאילו הם כבר ידועים. ושנית, הוא שם לב שניתן להסיק על פולינום בהסתמך על התמורות של שורשיו, בפרט האם הוא נשאר אינוואראנטי תחת תמורות אלו. אלא שלעומת משמעותו המקובלת של המונח כיום, דהיינו אינווראנטיות נומרית, לגרנג' מחפש אינווריאנטיות פורמלית של ממש.

על עבודתו זו של לגרנג' הסתמך פאולו רופיני כשהוכיח, ב-1799, את חוסר היכולת למצוא פתרון אלגברי לפולינום כללי ממעלה חמישית. לעומת לגרנג', שהסתכל על רק על השפעת התמורות על שורשי הפולינום, אלא חקר גם את התמורות עצמן, אם כי התייחסותו אליהן שונה מאוד מזו המודרנית. (אבל גם הוא נתן, בין 1824 ל-1828 מספר הוכחות לאי-קיום פתרון, אולם היא שונה מהקו שהתוו לגרנג' ורופיני, בכך שהיא מתבסת על חישובים ישירים ומסובכים, שבוקרו ככאלו גם בזמנו שלו.)

עוד מקור השפעה ברור על גלואה, פרט ללגרנג', הוא קושי. במאמר מ-1815[1] המרחיב את אחת מתוצאותיו של רופיני, הוא מתחיל לחקור תמורות כתמורות, ולא רק את השפעתן על שורשי הפולינום. אלא שאף על פי שהוא מתעניין בתמורות עצמן, ולא רק בסידורים שהם משרות, הוא נותן את השם *permutations* דווקא

1. בעל השם הארוך "Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme".

לסידורים השונים, וקורא בשם *substitutions* לתמורות הנובעות מסידורים אלו. זוהי גם הטרמינולגיה שגלואה ישתמש בה בחיבורו שלו.

"Memoir sur les conditions de résolubilité des équations par radicaux"

המאמר נפתח בכמה הגדרות "כולן כבר ידועות"[2]. ראשית, הוא קורא לערך נתון "רציונלי" אם הוא ביטוי אלגברי במספרים הרציונליים ובאוסף של ערכים שצורפו אליהם, בפרט, מקדמי הפולינום הנתון. במונחים מודרניים, גלואה מציג כאן הרחבה של שדה הרציונלים $\mathbb{Q}$, שתשמש כשדה הבסיס. נסמנו F.

הוא ממשיך ומגדיר *substitutions* ו-*permutations* כמו אצל קושי, ולכן הוא מדבר על חבורות של הסידורים (תמורות, בלשונו), כאשר ההחלפות נובעות מהן[3]. אם כי כבר בפתיחה הוא מדגיש כי החשיבות העיקרית היא בהחלפות עצמן, ולא בסידורים. בפרט, לאחר הבניה של החבורה המוכרת היום כ"חבורת גלואה", הוא חוזר ומדגיש:

> "ברור כי בחבורת התמורות בה מדובר, סידור האותיות אינו חשוב, אלא רק ההחלפות של האותיות שבאמצעותן עוברים מתמורה אחת לשניה"[4]

חשוב גם לציין מה הוא אינו מגדיר—פרט להערה כי חבורה של סידורים סגורה להרכבה של ההחלפות שהיא משרה, גלואה לא מגדיר חבורה כלל!

לאורך כל ההוכחות הבאות נדרש לפולינום פריד כלשהו ממעלה m, שמקדמיו בשדה הבסיס. נסמן פולינום זה ב-p. בטרמינולגיה מודרנית, נסתכל על שדה הפיצול E של פולינום זה, כהרחבת גלואה של F שבה אנו מסתכלים.

כעת, גלואה מציג שתי למות הטוענות כי ל-p כנ"ל קיים ביטוי V בשורשי הפולינום, כך שאין שתי תמורות של השורשים שערכו תחת פעולתן ערכו של V זהה (למה 2).

יתרה מזו, ניתן לבטא את כל שורשי p כביטויים רציונליים ב-V (למה 3).ניתן להסתכל על טענה זו כגרסה של המשפט המודרני הקובע כי הרחבה סופית ופרידה היא פשוטה[5], אלא שבעוד שההוכחה המודרנית מנצלת את תכונת הסגירות של השדות, גלואה משתמש בתכונות של הפולינומים הסימטריים[6].

כעת, ממשיך גלואה, אם נציג את V כנ"ל כשורש של פולינום אי פריק (בניסוח מודרני, זה יהיה הפולינום המינמלי של ההרחבה $E=F(V)$), נסמן את שורשי הפולינום ב- $V_1, V_2, \ldots$. וניקח את מהלמה הקודמת את

---

2. Edwards, Galois Theory, עמ' 101.
3. בהמשך נשתמש פעם בתיאור של חבורה כאוסף סידורים המשרים תמורות ופעם כאוסף תמורות, על פי ההקשר, אך ברור כי שני המונחים מקבילים. בכל מקרה, למען הבהירות, בהמשך (פרט לציטוט ישיר) המילה ""תמורה" תשמש במובנה המודרני, ו"סידור" במובן אליו גלואה התכוון.
4. Edwards, Galois Theory, עמ' 106.
5. אם כי אצל גלואה הטענה כללית פחות, כמובן.
6. על הוכחה זו ציין פואסון כי היא לוקה בחסר, אך הוכחה אחרת ניתנה כבר ע"י לגרנג'. בתגובה, גלואה מציין "*On Jugera*". לדעתי, הצדק כאן עם פואסון—גלואה נותן כאן לא יותר מסקיצה, אם כי אין זה מסובך מדי להרחיב אותה להוכחה מלאה.

הפונקציה ϕ הנותנת את השורש a של הפולינום p כביטוי של V_1, ז"א $\phi(V_1) = a$, אזי עבור ϕ כנ"ל, לכל j, $\phi(V_j)$ הוא שורש של p גם כן (למה 4).

כעת הוא פותח ומגדיר את "חבורת גלואה" באופן הבא:

> "טענה 1. תהי משוואה ב-m שורשים, $a,b,c,...$. תמיד קיימת חבורת של תמורות של האותיות $a,b,c,...$, בעלת התכונות הבאות:
>
> 1. כל פונקציה [ביטוי] אינווריאנטית* תחת ההחלפות של חבורה זה תהיה ידועה רציונלית;
>
> 2. ולהפך, כל פונקציה [ביטוי] בשורשים שניתן לחשב בצורה רציונלית יהיה אינווריאנטי תחת החלפות אלו.
>
> * כאן אנו קוראים לפונקציה אינווראנטית לא רק אם צורתה אינה משתנה ע"י ההחלפות של השורשים, אלא גם אם ערכה הנומרי אינו משתנה ... כשאנו אומרים שפונקציה היא ידועה רציונלית, כוונתנו שניתן לבטא את ערכה הנומרית כביטוי רציונלי במקדמי המשוואה והערכים שצורפו אליה"[7].

נרצה להראות כי ההגדרה הזו מתיישבת עם ההגדרה המקובלת כיום לחבורת גלואה, דהיינו, שבהנתן הרחבה נורמלית ופרידה E/F, נגדיר את חבורת גלואה להיות אוסף האוטומרפיזמים של E שהם העתקות הזהות על F (קל לראות כי אוסף כזה הוא אכן חבורה).

לשם כך, נשים לב קודם כל שאם נסתכל על ההרחבה המוסיפה את כל שורשי הפולינום לשדה הבסיס, כפי שעושה זאת גלואה במובלע, אזי היא נורמלית, וכיוון ש-p נבחר להיות פריד, ההרחבה הזו היא אכן "הרחבת גלואה".

E הוא שדה פיצול, לכן הוא נוצר ע"י הוספת שורשי p לשדה הבסיס, $E = F(\alpha_1, \ldots, \alpha_m)$, ולכן כל אוטומורפיזם על E/F נקבע באופן יחיד ע"י פעולתו על השורשים $\{\alpha_i\}$, כך שניתן להסתכל עליו באופן טבעי כתמורה בשורשים.

בפרט, כיוון שאוטומורפיזם כזה ישאיר את כל איברי שדה הבסיס ("ערכים הידועים רציונלית") במקומם, תנאי 2 של גלואה יתקיים, ואלו בדיוק האיברים שישארו במקום ע"י אוסף כל האוטמורפיזמים הללו, ולכן הם מקיימים את תנאי 1 של גלואה.

לכן, אם נסתכל על החבורה שגלואה מגדיר כאוסף ההחלפות שהיא משרה (ולא אוסף הסידורים), הרי שהחבורה הנ"ל איזומורפית לחבורת שגלואה מגדיר, וניתן להתייחס אל שתיהן כאותה החבורה ממש.

כהוכחה שלו לטענה לעיל, גלואה בונה את החבורה בפועל: בהנתן $\{V_i\}_{i=1}^n$ כמתוארות לעיל, ואוסף פונקציות רציונליות $\{\phi_i\}_{i=1}^m$ כך ש-$\phi_i(V_1) = \alpha_i$, עבור $\{\alpha_i\}$ שורשי p (קיומן של הפונקציות הללו מובטח מלמה 3), הוא לוקח את החבורה להיות n הסידורים הבאים:

$$\begin{matrix} \phi_1(V_1) & \phi_2(V_1) & \phi_3(V_1) & \ldots & \phi_m(V_1) \\ \phi_1(V_2) & \phi_2(V_2) & \phi_3(V_2) & \ldots & \phi_m(V_2) \\ \vdots & & & & \vdots \\ \phi_1(V_n) & \phi_2(V_n) & \phi_3(V_n) & \ldots & \phi_m(V_n) \end{matrix}$$

נזכור ש-n היא מעלת הפולינום המינמלי של ההרחבה, ולכן נקבל כי סדר החבורה שווה למימד ההרחבה.

גלואה לוקח את היות הנ"ל חבורה של סידורים על השורשים באופן טבעי, ואינו מראה שכל שורה היא

---

7. Edwards, Galois Theory, עמ' 105.

אכן סידור מתאים, או שהאוסף הנ"ל אכן סגור להרכבות של ההחלפות שהוא משרה (אף על פי שהוא ציין שחבורה צריכה לקיים זאת). אף על פי שהוא מציין שהחשיבות היא להחלפות בלבד, ולא לכתיבת הסידורים, הוא אינו מציין, או מראה, כי החבורה הזו היא היחידה המקיימת את הדרוש, כך שניתן לדמיין שבחירת V שונה תתן חבורה שתשרה החלפות שונות (אע"פ שבפועל זה לא כך).

ההוכחה שהוא כן מציע היא הבאה: בהנתן פולינום q בשורשים שערכו אינווריאנטי תחת ההחלפות של החבורה, נכתוב אותו כפולינום ψ ב-V_1 [הוא לא מציין, אך זו תוצאה מלמה 3 לעיל]. כעת נקבל:

$$\psi(V_1) = \psi(V_2) = \psi(V_3) = \cdots = \psi(V_n)$$

ומכאן, גלואה ממשיך, ניתן למצוא את ערך הפולינום q באופן רציונלי.

הסיבה המלאה למסקנה זו (שהוא אינו מציין), היא שמכאן ניתן לכתוב את הפולינום כביטוי סימטרי ב-V_i (למשל, $\frac{1}{n}\sum \psi(V_i)$). נזכור כי V_i הם שורשי פולינום עם מקדמים ב-F ולכן, כתוצאה מהמשפט היסודי של הפולינומים הסימטריים, ניתן לכתוב אותו כפולינום עם מקדמים בשדה F.

ולהפך: אם פולינום q בשורשים ניתן לחישוב רציונלי, ז"א ערכו בשדה הבסיס, נכתוב את אותו כפולינום ב-V_i, כיוון שלא יתכן שלביטוי ב-F יהיה מחלק משותף עם הפולינום המינמלי היוצר את V, שאז בפרט הוא יהיה פריק, בסתירה להנחה, ולכן q לא תלוי בשורשים, ובפרט לא משתנה תחת ההחלפות בהם.

נזכר כעת בניסוח המודרני של המשפט היסודי של תורת גלואה:

יהא E שדה הפיצול של פולינום פריד עם מקדמים בשדה F. אזי

א' כל שדה ביניים $F \subset B \subset E$ הוא שדה השבת של תת חבורה $H<\mathrm{Gal}(E/F)$, ולחבורות זרות מתאימים שדות זרים.

ב' בפרט, שדה ביניים B מהווה הרחבה נורמלית של F אסם חבורת גלואה המתאימה לו נורמלית ב-$\mathrm{Gal}(E/B)$.

ג' לכל שדה ביניים B, מימד ההרחבה B/F היא אינדכס החבורה המתאימה לו, ומימד ההרחבה E/B היא סדר החבורה הנ"ל.

ההוכחה המודרנית ארוכה למדי, אבל מסתמכת בעיקר על משפט שזכה להקרא אחרי ארטין, וקובע כתוצאה מהסתכלות על ההרחבה כמרחב וקטורי מעל שדה הבסיס, כי אם F הוא שדה השבת של חבורת אוטומורפיזמים של E, אזי סדר החבורה שווה לדרגת ההרחבה.

כדי להראות כיצד המשפט היסודי נובע מהמאמר המקורי של גלואה, נשים לב שמטענה 1 אצלו, הרי שחבורת גלואה של הרחבה של פולינום מעל שדה B קובעת בדיוק את B כשדה השבת שלה, ולכן נקבל את אל"ף. מבניית החבורה אצל גלואה, מספר אבריה הוא כמעלת הפולינום המינמלי, ולכן כמימד ההרחבה. את החלק השני של גימ"ל, על אינדכס החבורה, ניתן להסיק מתוך שיקולי מימד של שדות-וקטוריים (כפי שהדבר נעשה בגרסה המודרנית של ההוכחה).

כדי להוכיח את חלק בי"ת, נדרש לטענות הבאות של גלואה:

"טענה 2. אם מצרפים למשוואה הנתונה את השורש r של משוואת עזר בלתי-פריקה [ממעלה p]

1. תתכן אחת משתי האפשרויות: או שהחבורה של המשוואה לא תשתנה; או שהיא תתחלק ל-p חבורות, כל אחת מהן שייכת למשוואה המתאימה לצרוף אחד משורשי משוואת העזר;

2. לחבורות אלו תהייה התכונה הראויה לציון שניתן יהיה לעבור מאחת לשניה ע"י הפעלת אותה החלפה של האותיות על כל התמורות של הראשונה

.... טענה 3. אם מצרפים למשוואה את כל שורשיה של משוואת עזר, אזי החבורות מטענה 2 יהיו בעלות התכונה שכל אחת מהן מכילה את אותן ההחלפות"[8]

בעוד שלטענה 3 גלואה לא מציג הוכחה כלל[9], לטענה 2 הוא מציג הוכחה חלקית, בה מופיע ההערה המפורסמת "יש פרט שצריך השלמה בהוכחה זו. אין לי זמן לכך"[10] ששורבטה ערב הדו-קרב שהוביל אל מותו.

ההוכחה החלקית של טענה 2 מסתמכת על התבוננות בגורמים אליהם מתפרקת V לאחר הוספת אחת משורשיה, ושוב, ביטויים כפונקציות סימטריות של שורשיה האחרים של משוואה העזר.

נשים לב כי אם הרחבה היא נורמלית, הרי שמצרפים את כל השורשים, ולכן מתקיימת טענה 3. גלואה מסיק מכאן כי בכל אחת מהחבורות שנוצרות, התמורות, ביחס לסידור הבסיסי, זהות. לכן הן צמודות זו לזו, ולכן חבורת גלואה של ההרחבה המבוקשת נורמלית. ומכאן חלק ב"ת של המשפט היסודי, הגורס כי להרחבה נורמלית תהא חבורה נורמלית (ומהיות ההתאמה בין הרחבות וחבורות הפיכה, הרי שגם הכיוון השני קיים), ולכן חלקיו העיקריים של המשפט היסודי מוכחים כאן.

לסיכום הפרק הזה של המאמר, גלואה מנסח תשובה לשאלה באילו מקרים יש לפולינום פתרון ע"י רדיקלים: לשם בניית פתרון שכזה כך נדרש להוסיף בכל פעם לאוסף הערכים הידועים רציונליות רדיקל נוסף, ובכדי שהפולינום יהיה פתיר, נרצה שנוכל להוסיף רדיקלים כך שחבורת גלואה תקטן בכל פעם, עד שישאר בה רק סידור אחד של האיברים; כיוון שברגע שפולינום פתיר, כל ערך של שורשיו ידוע רציונלית.

לכן, אם ניתן בכל פעם לחלק את החבורה של המשוואה ל-k חבורות של סידורים בהתאם לטענה 3 לעיל, כלומר, למצוא בה תת-חבורה נורמלית לא-טריוואלית, הרי שעל ידי הוספת שורש k-י לערכים הידועים, נצמצם את חבורת גלואה.

כדוגמא, גלואה מתאר את החבורות הנוצרות ע"י הפתרון של הפולינום הכללי ממעלה רביעית.

שאר המאמר נושא את הכותרת "יישומים למשוואות בלתי פריקות ממעלה ראשונית", ומקוצר המקום והנושא, הוא לא יידון כאן. אם כי מהכותרת שגלואה נתן לו, ברור שכמו ממשיכיו המודרניים, גלואה מתייחס למציאת התנאים על פתרון פולינומים כיישום של התורה, ולא כמטרה העיקרית שלה.

8. Edwards, Galois Thoery, עמ' 107-106.
9. גרסה מוקדמת יותר של המאמר כוללת גרסה שונה שלה, עם הוכחה חלקית.
10. שם.

סיכום

לאחר קריאה של גלואה, ניתן לראות שבעוד שהוא היה אבסטרקטי יותר מקודמיו, והתעניין פחות בשאלה של פתרון משוואות כמו בתכונות של השורשים עצמם, הגישה שהוא מציג היא עדיין קונסטרוקטיבית; אף על פי שלא ניתן לבנות ממנה בקלות פתרונות לפולינום, עדיין הוא בונה ממש את החבורה.

לא רק שבניסוח המודרני קיום החבורה מוצג ללא בניה של ממש, אלא שגם הפולינום שיוצר את ההרחבה, המשחק תפקיד חשוב אצל גלואה, משחק כאן רק תפקיד משני.

כך שהגרסה המודרנית הופכת את עבודתו של גלואה מעבודה לעוד יותר אבסטרקטית, ומנתקת את עבודתו של גלואה ממקורה בחקר הפולינומים אל חקר השדות.

בהסתכלות על טכניקות ההוכחה, הן שונות למדי: זו של גלואה מסתמכת בעיקר על הפולינומים הסימטריים, בעוד שהגרסה המודרנית מעדיפה להסתמך על תכונות של חבורות ומרחבים וקטוריים, ובכל זאת, ניתן להשתמש בטכניקה המקורית גם כדי להסיק את הגרסה המודרנית.

ביבליוגרפיה

Artin, Emil, *Galois Theory (2nd Edition*), Notre Dame, Edwards Brothers, 1946.

Edwards, Harold M., *Galois Theory*, Springer-Verlag, New York, 1984.

Kiernan, B.M., The Development of Galois Theory from Lagrange to Artin, *Archive for History of Exact Science* **8** (1971), pp 40-154.

Nový, Luboš, *Origins of Modern Algebra* (trans. Jaroslav Tauer,) Nordhoff International Publishing, Leyden, 1973.

Sørensen, Henrik Kragh, Niels Henrik Abel and the theory of equations, Appendix of progress report, Institut for Videnskabshistorie, Aarhus Universitet, 1999. Online at *www.henrikkragh.dk/pdf/part199911g.pdf*.