מבנים אלגבריים 2

29 באוקטובר 2015

.

מבוסס על הרצאות פרופ' אודי הרושובסקי
בקורס "מבנים אלגבריים 2" (80446)
האוניברסיטה העברית, סמסטר ב' 2014
להערות: *nachi.avraham@gmail.com*

נחי

תודה לכל מי ששלח הערות ותיקונים, ובמיוחד ל:
נעמה בויאר, גיא גולדברג, אלעד גולדפרב, הדר גורודיסקי, צחי טאוב, אלכס טוש, גל יונה, ענבל יפה, מאיה לשקוביץ, רון מור, אוריאל עצמון, מעיין קפלן, עודד רימון ורעות שאבו

תוכן עניינים

I חוגים **3**

1 חוגים כלליים 3

1.1 חוג האנדומורפיזמים 4

1.2 מודולים 5

1.3 משפט קיילי 6

2 חוגים קומוטטיביים 6

2.1 חוגים אוקלידיים 7

2.2 אידאל נוצר 7

2.3 מיון חוגים קומוטטיביים לפי מבנה האידאלים בהם 8

2.4 אי־פריקות וראשוניות 9

2.5 פריקות 10

2.6 חוג השלמים של גאוס $\mathbb{Z}[i]$ 12

2.6.1 ההפיכים של $\mathbb{Z}[i]$ 13

2.6.2 הראשוניים של $\mathbb{Z}[i]$ 13

3 חוגי פולינומים 15

3.1 הלמה של גאוס 16

3.2 הקריטריון של אייזנשטיין 19

4 משפט המבנה למודולים נוצרים־סופית 20

II שדות **23**

5 הרחבת שדות 23

5.1 איברים אלגבריים 24

5.1.1 המספרים האלגבריים 26

6 הומומורפיזם של שדות 27

7 בנייה באמצעות סרגל ומחוגה 31

8 נגזרת פורמלית 34

III תורת גלואה **36**

9 הרחבות נורמליות 36

10 התאמת גלואה 39

11 הקשר בין נורמליות בחבורות ובשדות 43

12 חבורת גלואה כבסיס למרחב ווקטורי 44

13 הרחבות ציקליות 45

14 פתירות 46

14.1 פתירות בעזרת רדיקלים 47

14.1.1 השדה הנוצר של הפולינומים הסימטריים היסודיים 51

חלק I
חוגים

1 חוגים כלליים

הגדרה: **חוג** הוא $(R,+,\cdot,0,1)$ כאשר R קבוצה לא ריקה, $0,1\in R$ איברים מיוחדים, וכן $+,\cdot$ פעולות דו־מקומיות $R\times R\to R$, כך שלכל $a,b,c\in R$ מתקיים:

1. **תכונות הקשורות לפעולת החיבור:**
   (א) **קומוטטיביות של החיבור:** $a+b=b+a$
   (ב) **אסוציאטיביות של החיבור:** $(a+b)+c=a+(b+c)$
   (ג) **איבר האפס:** קיים איבר $0\in R$ המקיים $a+0=a$
   (ד) **איבר נגדי לחיבור:** קיים $-a\in R$ כך שמתקיים $a+(-a)=0$
2. **תכונות הקשורות לפעולת הכפל:**
   (א) **אסוציאטיביות של הכפל:** $(a\cdot b)\cdot c=a\cdot(b\cdot c)$
   (ב) **איבר יחידה:** קיים $1\in R$ כך שמתקיים $a\cdot 1=1\cdot a=a$
3. **תכונות הקשורות בין החיבור והכפל:**
   (א) **דיסטריבוטיביות משמאל:** $(a+b)\cdot c=a\cdot c+b\cdot c$
   (ב) **דיסטריבוטיביות מימין:** $a\cdot(b+c)=a\cdot b+a\cdot c$

הערה: לעתים מגדירים חוג ללא איבר יחידה.

הערה: במונחים כלליים יותר, $(R,+,\cdot,0,1)$ הוא חוג אמ"מ $(R,+,0)$ היא חבורה חיבורית קומוטטיבית,[1] וכן גם $(R,\cdot,1)$ הוא מונואיד (כלומר $\cdot$ פעולה דו־מקומית אסוציאטיבית, ו-1 איבר יחידה כפי שהזכרנו לעיל).

הגדרה: בהינתן חוג R ותת־קבוצה $I\subset R$, אומרים כי I הוא **אידאל** מעל R, אם מתקיים כי $(I,+,0)$ היא תת־חבורה חיבורית של $(R,+,0)$, וכן מתקיימת סגירות לכפל סקלרי. כלומר לכל $r\in R$ ולכל $i\in I$ מתקיים $r\cdot i\in I$ וכן $i\cdot r\in I$.

הגדרה: בהינתן I אידאל בחוג R, מתקבל **חוג־מנה** $R/I=:\{r+I|r\in R\}$ תחת הפעולות הבאות:

$$(r+I)+(s+I)=(r+s)+I$$

$$(r+I)\cdot(s+I)=r\cdot s+I$$

[1] למעשה אין צורך לדרוש את הקומוטטיביות, כי היא נובעת מתכונות החוג:

$$x+(x+y)+y=x(1+1)+y(1+1)=(x+y)(1+1)=(x+y)+(x+y)=x+(y+x)+y$$

וכעת על־ידי שימוש בקיום הנגדי לחיבור נוכל לצמצם ולקבל $x+y=y+x$.

הקדמה: שתי המשפחות היסודיות של חבורות הן החבורות האבליות וחבורות הסימטריות, שהללו האחרונות כמעט תמיד אינן אבליות.

באופן כללי, לכל חבורה G וקבוצה Ω ניתן להגדיר **פעולה** של G על Ω על־ידי הומומורפיזם מהצורה $\rho : G \to Sym\left(\Omega\right)$, כאשר $Sym\left(\Omega\right)$ היא חבורת התמורות של איברי Ω. כלומר זו העתקה $G \times \Omega \to \Omega$ מהצורה $\left(g,x\right) \mapsto \rho\left(g\right)\left(x\right)$.

משפט קיילי קבע שלכל חבורה G קיימת קבוצה Ω כך ש-G משתכנת בתוך $Sym\left(\Omega\right)$. כלומר קיים הומומורפיזם $\rho : G \to Sym\left(\Omega\right)$ שהוא חח"ע.

נרצה למצוא אנלוגים למושגים אלו בחוגים. נראה שכפי שחבורה G "חיה מעל" קבוצה Ω כלשהי, האנלוגיה לחוגים תהיה שחוג "חי מעל" החבורה האבלית שלו. נראה עוד כי "חוג האנדומורפיזמים" על החבורה האבלית של החוג, שמיד נגדיר, הוא האנלוג של החבורה Sym, וכי פעולה של חוג על "מודול", שנגדיר בהמשך, היא האנלוג לפעולה של חבורה על קבוצה.

לבסוף נראה את משפט קיילי לחוגים, לפיו כל חוג משתכן בתוך "חוג האנדומורפיזמים" של חבורה אבלית.

1.1 חוג האנדומורפיזמים

הגדרה: תהי A חבורה אבלית, אזי מגדירים $\text{End}\left(A\right) =: \text{Hom}\left(A,A\right)$. כלומר זהו אוסף ההומומורפיזמים מהצורה $\rho : A \to A$. הומומורפיזם כזה מכונה **אנדומורפיזם**, ו-$\text{End}\left(A\right)$ מכונה **חוג האנדומורפיזמים**.

הגדרה: נגדיר את $\text{Hom}\left(A,A\right)$ כחבורה אבלית באופן כללי יותר.

בהינתן A,B חבורות אבליות, נגדיר פעולה $+$ על הקבוצה $\text{Hom}\left(A,B\right)$ באופן נקודתי. כלומר $\left(f+g\right)\left(a\right) = f\left(a\right) + g\left(a\right)$ לכל $a \in A$.[2]

תחת הפעולה $+$ שהגדרנו מתקבלת חבורה $\text{Hom}\left(A,B\right)$, כאשר איבר ה-0 הוא ההומומורפיזם הקבוע $f = 0$.

הגדרה: נגדיר את $\text{Hom}\left(A,A\right)$ כמונואיד.

בהינתן A חבורה אבלית, נגדיר פעולה $\cdot$ על ידי הרכבת פונקציות. כלומר $\left(f \cdot g\right)\left(a\right) = \left(f \circ g\right)\left(a\right) = f\left(g\left(a\right)\right)$, לכל $a \in A$.[3]

תחת פעולת ההרכבה שהגדרנו מתקבל מונואיד $\text{End}\left(A\right)$, כאשר איבר היחידה הוא הומומורפיזם הזהות $f = Id$.

מסקנה: מצאנו שבהינתן חבורה אבלית A, מה שהגדרנו $\left(\text{End}\left(A\right), +, \circ, 0, Id\right)$ הוא חוג.

נימוק: $\left(\text{End}\left(A\right), +, 0\right)$ היא חבורה חיבורית כפי שראינו, והיא קומוטטיבית מאבליות A.

$\left(\text{End}\left(A\right), \circ, Id\right)$ הוא מונואיד, שכן הוא אסוציאטיבי כפי שהרכבת פונקציות אסוציאטיבית מהגדרתה, וקל לראות כי $f = Id$ הוא איבר יחידה העונה לדרישות.

נותר להראות דיסטריבוטיביות מימין ומשמאל:

[2] יש להראות כי $f + g \in \text{Hom}\left(A,B\right)$.
[3] יש להראות כי $f \circ g \in \text{End}\left(A\right)$.

- דיסטריבוטיביות משמאל נובעת באופן כללי מהגדרת הרכבה של פונקציות:

$$((f+g)\circ h)(a)=(f+g)(h(a))=f(h(a))+g(h(a))=f\circ h(a)+g\circ h(a)$$

- דיסטריבוטיביות מימין נובעת מכך שמדובר בהומומורפיזם (המעבר הקריטי הוא השוויון השני):

$$(f\circ(g+h))(a)=f(g(a)+h(a))=f(g(a))+f(h(a))=f\circ g(a)+f\circ h(a)$$

■

1.2 מודולים

הגדרה: אם R חוג ו-A חבורה אבלית עם הומומורפיזם מהצורה $\rho:R\to\mathrm{End}(A)$, אומרים כי A **מודול** מעל R.

תיאור אחר: בהינתן R חוג ו-A חבורה אבלית והומומורפיזם $\rho:R\to\mathrm{End}(A)$, נגדיר העתקה $\tilde{\rho}:R\times A\to A$ להיות $\tilde{\rho}(r,a)=\rho(r)(a)$. באופן שקול, גם הומומורפיזם זה מגדיר את A כמודול מעל R.

כדאי לחשוב מדוע $\rho,\tilde{\rho}$ מבטאים בעצם את אותה האינפורמציה.

סימון: בדיונים בהם יהיה ברור מהו ההומומורפיזם ρ, לעתים במקום לכתוב $\rho(r)(a)$ נכתוב $r.a$ או גם ra.

תכונות של מודולים:

1. $r(a+b)=ra+rb$

הוכחה: מכך שהטווח של ρ הוא חוג האנדומורפיזמים, $\rho(r)$ הוא אנדומורפיזם כלשהו. לכן $\rho(r)(a+b)=\rho(r)(a)+\rho(r)(b)$.

2. $(r+s)a=ra+sa$

הוכחה: נחשב:

$$\rho(r+s)(a)=(\rho(r)+\rho(s))(a)=\rho(r)(s)+\rho(s)(a)$$

כאשר השוויון הראשון נובע מכך ש-ρ הומומורפיזם של חוגים, והשוויון השני נובע מהגדרת חיבור נקודתי של פונקציות.

3. $(rs)(a)=r(s(a))$

הוכחה: מכיוון ש-ρ הומומורפיזם של חוגים, נובע שמתקיים $\rho(rs)=\rho(r)\cdot\rho(s)=\rho(r)\circ\rho(s)$, כאשר השוויון הראשון נובע מהיות ρ הומומורפיזם של חוגים, והשוויון השני נובע מהגדרת הכפל בחוג $\mathrm{End}(A)$.

4. $0a=0$

5. $1a=a$

הערה: מתכונות אלה נובע שמושג המודול מכליל את מושג מרחב הווקטורי, שהוא למעשה מודול מעל חוג חילוק קומוטטיבי, דהיינו שדה.

1.3 משפט קיילי

לכל חוג R קיימת חבורה אבלית A, כך ש-R איזומורפי לתת־חוג של $\mathrm{End}\,(A)$.

הוכחה: בהינתן R, נבחר את A להיות $(R,+,0)$. כלומר $A=R$ כקבוצה, וכן הפעולה $+$ היא הפעולה בחוג R, ו-0 הוא איבר האפס ב-R.

נגדיר העתקה $\rho:R\to\mathrm{End}\,(A)$ להיות $\rho\,(r)\,(a)=r\cdot a$, כאשר $\cdot$ היא הכפל המוגדר בחוג R.

נראה כי ρ היא שיכון של R בתוך $\mathrm{End}\,(A)$. לשם כך יש להראות את העובדות הבאות:

1. ρ הומומורפיזם של חוגים.

   נימוק: מדיסטריבוטיביות משמאל בחוג R נובע $\rho\,(r+s)=\rho\,(r)+\rho\,(s)$.
   מאסוציאטיביות הכפל בחוג R נובע $\rho\,(rs)=\rho\,(r)\circ\rho\,(s)$.
   כמו־כן קל לראות כי $\rho\,(1)=Id$ וכן $\rho\,(0)=0$ (כלומר הומומורפיזם האפס).

2. $\rho\,(r)\in\mathrm{End}\,(A)$. כלומר שתמונת ρ היא אכן $\mathrm{End}\,(A)$, ובאופן כללי ידוע כי תמונה של הומומורפיזם היא תת־חוג.

   נימוק: $\rho\,(r)\,(a+b)=\rho\,(r)\,(a)+\rho\,(r)\,(b)$ מהדיסטריבוטיביות בחוג R.

3. ρ חח"ע.

   נימוק: מספיק להראות ש-$\ker\,(\rho)$ טריוויאלי. יהי $r\in\ker\,(\rho)$, כלומר $\rho\,(r)=0$. כלומר $r\cdot a=0$ לכל $a\in R$, ולכן בהכרח $r=0$. מכאן כי $\ker\,(\rho)=\{0\}$.

כעת נתבונן בתמונה של ρ בתוך $\mathrm{End}\,(A)$, שנסמן $\rho\,(R)$. קל לראות כי R איזומורפי על ידי ρ לתת־חוג $\rho\,(R)$.[4] ■

הערה: כל אידאל הוא תת־מודול של החוג. ראשית הוא תת־חבורה חיבורית מהגדרתו, וכמו־כן ההומומורפיזם $\rho:R\to\mathrm{End}\,(A)$ ל-$A=(R,+,0)$ מגדיר כל חוג R כמודול מעל עצמו, ולכן כל אידאל ב-R הוא תת־מודול של המודול R.

2 חוגים קומוטטיביים

הגדרה: חוג R נקרא **קומוטטיבי**, אם לכל $x,y\in R$ מתקיים $x\cdot y=y\cdot x$ ביחס לכפל בחוג.

הגדרה: חוג R נקרא **חוג חילוק**, אם לכל איבר בו קיים איבר הופכי ביחס לכפל בחוג. כלומר לכל $x\in R$ קיים $y\in R$ כך שמתקיים $xy=1$.

הגדרה: חוג חילוק קומוטטיבי נקרא **שדה**.

הגדרה: חוג קומוטטיבי R נקרא **תחום שלמות**, אם אין בו מחלקי אפס. כלומר לכל $x,y\in R$, אם $x\neq 0$ וגם $y\neq 0$, אז $x\cdot y\neq 0$.

כך למשל החוג $\mathbb{Z}/4\mathbb{Z}$ אינו תחום שלמות, שכן בו $2\cdot 2=0$.

הערה: אם חוג אינו תחום שלמות הוא לא יכול להיות חוג חילוק, שכן אם יש בו מחלקי אפס $xy=0$, $x,y\neq 0$, אז $x\,(yz)=(xy)\,z=0\cdot z=0$ לכל $z\in R$, ולכן ל-x או y אין הופכי.

[4] מבחינה פורמלית ρ עצמו אינו איזומורפיזם, אלא הצמצום שלו.

הערה: כל תחום שלמות משתכן בתוך שדה. ניתן לבנות שדה כזה באופן מפורש בדיוק באופן שבו בונים את שדה הרציונליים $\mathbb{Q}$ מתוך חוג השלמים $\mathbb{Z}$, והוא מכונה **שדה השברים**.

2.1 חוגים אוקלידיים

הגדרה: חוג R שהוא תחום שלמות נקרא **חוג אוקלידי**, אם יש בו **חלוקה עם שארית**.

כלומר, אם קיימת פונקציה $d : R\setminus\{0\} \to \mathbb{N}$ המקיימת שני תנאים:

1. לכל $x \in R$ מתקיים $d(x) \leq d(xy)$, לכל $y \in R$.
2. לכל $a, b \in R$, אם $b \neq 0$ אז קיימים $r, s \in R$ כך שמתקיים $a = sb + r$, ומתקיימת בדיוק אחת מהאפשרויות הבאות: $r = 0$ או $r \neq 0$ וגם $d(r) < d(b)$.

דוגמאות:

1. חוג השלמים $\mathbb{Z}$ עם הפונקציה $d(n) = |n|$ הוא חוג אוקלידי.
2. החוג $\mathbb{Z}[i] = \left\{a + bi | a, b \in \mathbb{Z},\, i^2 = -1\right\}$ (**חוג השלמים של גאוס**). נוכיח בהמשך שזה אכן חוג אוקלידי.
3. בהינתן שדה $\mathbb{F}$, חוג הפולינומים במשתנה יחיד מעליו מסומן $\mathbb{F}[x]$.

   זה חוג אוקלידי עם הפונקציה $d\left(\sum_{i=1}^{n} a_i x^i\right) = n$ עבור $a_n \neq 0$. כלומר לכל $p \in \mathbb{F}[x]$ מגדירים $d(p) = \deg(p)$.

2.2 אידאל נוצר

הגדרה: אם R חוג, אז **אידאל נוצר** על־ידי אוסף איברים ב-R הוא האידאל המינימלי שמכיל את כולם.

הגדרה שקולה: האידאל הנוצר של האוסף $\{a_1, ..., a_n\} \subset R$ היא האידאל $Ra_1 + ... + Ra_n$, כאשר לכל i, $1 \leq i \leq n$ מתקיים $Ra_i = \{ra_i | r \in R\}$. מסמנים זאת $(a_1, ..., a_n)$.

הוכחה: בהינתן $\{a_1, ..., a_n\} \subset R$, אם I הוא האידאל המינימלי שמכיל את הקבוצה הנ"ל אז קל לראות כי $(a_1, ..., a_n) \subset I$.

מצד שני, ניתן להראות כי $(a_1, ..., a_n)$ הוא אכן אידאל, וברור שהוא מכיל את $\{a_1, ..., a_n\}$, ולכן ממינימליות I נובע כי $I = (a_1, ..., a_n)$. ■

הערה: בהינתן מודול כלשהו M בחוג קומוטטיבי R, **תת־מודול** של M מוגדר כתת־קבוצה שלו, שסגורה תחת חיבור וכפל סקלרי.

הערה: אידאל הוא מקרה פרטי של תת־מודול, כאשר מסתכלים על R כמודול מעל עצמו. לכן לומר ש-I אידאל ב-R שקול לאמירה ש-I תת־מודול של R כמודול מעל עצמו.

טענה: בתחום שלמות שני איברים יוצרים את אותו מודול אם ורק אם הם חברים.[5]

[5] מגדירים כי $a, b \in R$ חברים, אם קיים $u \in R$ הפיך, כך ש-$a = bu$.

הוכחה: יהיו $a, b \in R$ ונניח כי $a \sim b$ ביחס החברות, כלומר יש $u \in R$ הפיך כך שמתקיים $a = bu$.

מהשוויון האחרון נובע כי $a \in (b)$, וקל לראות שגם $au^{-1} = b$ ולכן $b \in (a)$. מכאן כי $(a) = (b)$.

בכיוון שני, אם $(a) = (b)$ אז $a = bt$ וגם $b = as$ ל-$t, s \in R$ כלשהם. לכן $a = bt = ast$ ומכאן כי $st = 1$, כלומר s, t הפיכים ולכן $a \sim b$. ■

מסקנה: איבר יוצר של אידאל כמעט תמיד אינו יחיד. למשל $(a) = (-a)$, שכן $a \sim -a$.

2.3 מיון חוגים קומוטטיביים לפי מבנה האידאלים בהם

נמיין את החוגים הקומוטטיביים בהתאם למבנה האידאלים בהם.

1. **שדה:** חוג קומוטטיבי ופשוט. כלומר חוג קומוטטיבי R שבו יש שני אידאלים בלבד - $R, \{0\}$.[6]
2. **תחום ראשי:** תחום שלמות בו כל אידאל הוא אידאל ראשי. כלומר כל אידאל הוא מהצורה (a).
3. **חוג נתר:** תחום שלמות שבו כל אידאל נוצר־סופית.

משפט: כל חוג אוקלידי הוא תחום ראשי.

הוכחה: יהי R חוג אוקלידי ויהי I אידאל ב-R. אם $I = \{0\}$ אז $I = (0)$ ולכן נוצר על־ידי איבר יחיד. לכן נניח $I \neq \{0\}$.

נבחר $0 \neq a \in I$ כך שעבורו $d(a)$ הוא הערך המזערי. נוכיח שמתקיים $I = (a)$. קל לראות כי $(a) \subset I$. נראה את ההכלה ההפוכה.

יהי $b \in I$. מהיות R חוג אוקלידי נובע שניתן לחלק עם שארית, ולכן קיימים $r, s \in R$ כך שמתקיים $b = sa + r$ כאשר $d(r) < d(a)$.

מהיות I אידאל נובע כי $r = b - sa \in I$. מהיות $d(a)$ מזערי ב-I נובע שבהכרח $r = 0$, שכן $d(r) < d(a)$, ומכאן כי $b = sa$ ועל־כן $b \in (a)$, כלומר $I \subset (a)$. ■

דוגמה: יהי R תחום ראשי. לכל $c, d \in R$ קיים $a \in R$ כך שמתקיים $(c, d) = (a)$, שכן R ראשי. לכן מתקיים כי $a = rc + sd$ ל-$r, s \in R$ כלשהם.

לכל $a' \in R$ המקיים $a'|c$, $a'|d$ מתקיים $a'|rc + sd = a$. כלומר a הוא המחלק המקסימלי של c, d עד כדי חברות. נסמן אותו ב-$a = \gcd(c, d)$ (נשים לב שסימון זה מוגדר עד־כדי חברות).

משפט: יהי M R־מודול, אזי התנאים הבאים שקולים:

1. כל תת־מודול של M נוצר־סופית.
2. M מקיים את **תנאי השרשרת העולה**: <u>אין</u> שרשרת אינסופית של תתי־מודולים העולה ממש ביחס להכלה.

---

[6] חוג קומוטטיבי הוא שדה (כלומר גם חוג חילוק) אמ"מ הוא חוג פשוט:
אם R שדה, אז לכל איבר בו יש הופכי, ולכן כל אידאל שמכיל איבר שאינו 0 מכיל את 1, ולכן הוא החוג כולו.
אם R חוג קומוטטיבי ופשוט, אז לכל $a \in R$ האידאל הנוצר על־ידי a שנסמן aR הוא $\{0\}$ או R. אם $aR = \{0\}$ אז $a = 0$, ואם $aR = R$ אז בפרט יש $r \in R$ כך ש-$ar = 1$, כלומר ל-a יש הופכי.

3. לכל $\mathcal{Y}$ משפחה של תתי־מודולים שאינה ריקה, קיים איבר מירבי.
"מירבי" במובן זה שקיים $I \in \mathcal{Y}$ כך שלא קיים $J \in \mathcal{Y}$ המקיים $I \subsetneqq J$.

הוכחה:

$(1 \Leftarrow 2)$ נניח בשלילה שקיימת סדרה אינסופית עולה ממש של תתי־מודולים, שנסמן $I_1 \subsetneqq I_2 \subsetneqq \ldots$.

נגדיר $I = \bigcup_{n=1}^{\infty} I_n$. מכך שזו סדרה עולה ממש ביחס להכלה נובע כי I סגור לחיבור ולכפל סקלרי, כלומר הוא תת־מודול.[7] מההנחה נובע כי I נוצר־סופית, אז נסמן $I = (a_1, ..., a_n)$.

מהגדרת I נובע שקיים K מספיק גדול כך שמתקיים $\{a_1, ..., a_n\} \subset I_K$, ולכן $I \subset I_K \subsetneqq I_{K+1} \subsetneqq I$, וזו סתירה.

$(2 \Leftarrow 3)$ תהי $\mathcal{Y} \neq \emptyset$ משפחה של תתי־מודולים, ונניח בשלילה שאין בה איבר מירבי.

נבנה שרשרת אינסופית של תתי־מודולים שתעלה ממש ביחס להכלה באופן הבא: יהי $I_1 \in \mathcal{Y}$. הוא אינו מירבי ולכן יש $I_2 \in \mathcal{Y}$ כך שמתקיים $I_1 \subsetneqq I_2$. גם I_2 אינו מירבי ולכן יש $I_3 \in \mathcal{Y}$ כך שמתקיים $I_1 \subsetneqq I_2 \subsetneqq I_3$. הבנייה לא תיעצר אף פעם שכן ב-$\mathcal{Y}$ אין איבר מירבי, ולכן מצאנו שרשרת אינסופית של תתי־מודולים העולה ממש ביחס להכלה, בסתירה להנחה.

הערה: נשים לב שהשתמשנו באקסיומת הבחירה בהוכחת החלק האחרון, אולם אין חשיבות לבנייה ולכן זה לא מהותי.

$(3 \Leftarrow 1)$ יהי I תת־מודול ב-R. נגדיר את $\mathcal{Y}$ להיות אוסף תתי המודולים הנוצרים־סופית שמוכלים ב-I. אוסף זה אינו ריק כי $\{0\} \in \mathcal{Y}$.

מההנחה נובע שקיים $J \in \mathcal{Y}$ שהוא מירבי, והוא נוצר־סופית מהגדרת הקבוצה $\mathcal{Y}$. נוכיח כי $I = J$.

יהי $a \in I$. קל לראות כי תת המודול $J + (a)$ עדיין נוצר־סופית ומוכל ב-I, ולכן ממירביות J ב-$\mathcal{Y}$ נובע כי $J + (a) = J$.

בחרנו את $a \in I$ שרירותית, ולכן נובע כי $I = J + I = J$ (כאשר השוויון הראשון נובע מכך ש-$J \subset I$), ומכאן כי I נוצר־סופית. ■

2.4 אי־פריקות וראשוניות

בפרק זה נעסוק רק בתחומי שלמות. כלומר חוגים קומוטטיביים ללא מחלקי אפס.

הגדרה: יהי R תחום שלמות. אומרים כי $0 \neq p \in R$ לא־הפיך הוא **ראשוני**, אם לכל $a, b \in R$ מתקיים כי אם $p|ab$ אז $p|a$ או $p|b$.

הגדרה: יהי R תחום שלמות. אומרים כי $0 \neq p \in R$ לא־הפיך הוא **אי־פריק**, אם לכל $a, b \in R$ מתקיים כי אם $p = ab$ אז $p|a$ או $p|b$.

טענה: p אי־פריק $\iff$ אם $p = ab$ אז a הפיך או b הפיך, ולפיכך ביחס החברות $p \sim b$ או $p \sim a$ בהתאמה $\iff$ $(p) \lhd R$ הוא אידאל מירבי מבין האידאלים הראשיים (למעט האידאל הראשי $R = (1)$).

[7] שכן לכל $a, b \in I$ קיים N מספיק גדול כך ש-$a, b \in I_N$.

הוכחה: נראה ששני התנאים שקולים לאי־פריקות במובן שהגדרנו.

- נראה את השקילות לתנאי הראשון: בכיוון ראשון, אם p אי־פריק ו-$p=ab$, מהגדרת אי־פריקות נובע בלא הגבלת הכלליות, ולכן $p|b$ ללא הגבלת הכלליות, ולכן $pc=b$ ל-$c\in R$, ומכאן $p=ab=apc$. מכך ש-R הוא תחום שלמות, מהקומוטטיביות ומכך שאפשר לצמצם ב-p נובע $ac=1$, ומכאן כי a הפיך, ולכן $p\sim b$.

  בכיוון השני, בהינתן $p=ab$ ונניח ללא הגבלת הכלליות כי b הפיך, אז $bu=1$ ל-$u\in R$, ולכן $pu=abu=a$ ומכאן $p|a$.
- נראה את השקילות לתנאי השני:

למה: $a|b \iff (b)\subset(a)$. כלומר סדר החלוקה בין איברים הפוך מסדר ההכלה בין האידאלים הנוצרים על־ידם.

הוכחה: אם $a|b$ אז $b=ac$ ולכן $b\in(a)$. מצד שני, אם $(b)\subset(a)$ אז בפרט $b\in(a)$ ולכן קיים $c\in R$ כך ש-$b=ac$, כלומר $a|b$.

מכאן נובע שאם p אי־פריק זה אומר שאין לו מחלקים ממש (למעט $1\sim$), כלומר הוא מזערי בסדר החלוקה בין איברים. מכאן שהאידאל הנוצר על־ידו מירבי מבין האידאלים הראשיים (למעט $R=(1)$). ■

טענה: בתחום שלמות כל איבר ראשוני הוא אי־פריק.

הוכחה: יהי p ראשוני ונניח כי $p=ab$. בפרט $p|ab$ ולכן מראשוניות p נובע $p|a$ או $p|b$. ■

2.5 פריקות

הגדרה: תחום שלמות R נקרא UFD (תחום פריקות חד־ערכית; Unique Factorizaton Domain) אם לכל $0\neq a\in R$ לא־הפיך קיים פירוק יחיד לראשוניים עד כדי חברות. כלומר הוא ניתן להיכתב כמכפלה יחידה של ראשוניים עד כדי חברות.

למה: בתחום שלמות R, אם קיים פירוק לראשוניים אז הוא יחיד.

כלומר אם $p_1,...,p_n,q_1,...,q_m\in R$ ראשוניים כך שמתקיים $p_1\cdot...\cdot p_n=q_1\cdot...\cdot q_m$, אז $n=m$ וקיימת תמורה $\sigma\in Sym\left(n\right)$ כך ש-$p_i\sim q_{\sigma(i)}$ לכל $1\leq i\leq n$.

מסקנה: בפרט תחום ראשי שהוא תחום פריקות הוא גם UFD.

הוכחה: באינדוקציה על n.

אם $n=1$, כלומר $p=q_1\cdot...\cdot q_m$, אז מראשוניות p נובע כי הוא אי־פריק ולכן $p|q_1$ או $p|q_2\cdot...\cdot q_m$, וכפי שראינו זה אומר ש-q_1 הפיך או $q_2\cdot...\cdot q_m$ הפיך.

לא ייתכן ש-q_1 הפיך כי הוא ראשוני, ולכן בהכרח $q_2\cdot...\cdot q_m$ הפיך. כלומר יש $u\in R$ כך ש-$u\cdot q_2\cdot...\cdot q_m-1=0$ ולכן:

$$p\cdot u-q_1=u\cdot q_1\cdot q_2\cdot...\cdot q_m-q_1=q_1\left(u\cdot q_2\cdot...\cdot q_m-1\right)=0$$

מכאן כי $q_1=p\cdot u$, כלומר $m=1$ וכן $p\sim q_1$.

נוכיח ל-n כללי. נניח $p_1\cdot...\cdot p_n=q_1\cdot...\cdot q_m$, אזי $p_1|q_1\cdot...\cdot q_m$ ומראשוניות p_1 נסיק שקיים $1\leq k\leq m$ כך ש-$p_1|q_k$. כלומר $q_k=p_1\cdot u_1$ ל-$u_1\in R$. אבל q_k ראשוני ולכן אי־פריק, ומכאן כי u_1 הפיך (p_1 ראשוני ולכן לא הפיך) ולכן $p_1\sim q_k$.

R תחום שלמות ולכן נצמצם ב-q_k ונקבל כי $p_1 = u_1 \cdot q_k$ ... $p_2 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot \hat{q}_k \cdot \ldots \cdot$ $q_m \cdot u_1^{-1}$ (משמעות הסימון $\hat{q}_k$ היא שמסירים איבר זה מהמכפלה).

האיבר $q_m \cdot u_1^{-1}$ הוא עדיין ראשוני (באופן כללי, הכפלה של ראשוני באיבר הפיך משאירה ראשוני), ולכן מהנחת האינדוקציה נובע כי $n-1 = m-1$ וקיימת $\sigma \in Sym\left(n-1\right)$ כך ש-$p_i \sim q_{\sigma(i)}$ עבור $2 \leq i \leq n$. מכאן כי $n = m$, ואם נוסיף לתמורה σ את החילוף $(1k)$ נקבל תמורה ב-$Sym\left(n\right)$ כנדרש. ■

משפט: כל תחום ראשי הוא תחום פריקות חד־ערכית.

מסקנה: ראינו שכל חוג אוקלידי הוא תחום ראשי, ולכן הוא בפרט גם תחום פריקות חד־ערכית.

הוכחה: מבנה ההוכחה יהיה כך: (1) תחום ראשי הוא חוג נתר. (2) בחוג נתר לכל איבר קיים פירוק לאיברים אי־פריקים. (3) בתחום ראשי כל אי־פריק הוא ראשוני. מאלה המשפט נובע מידית.

למה 1: כל תחום ראשי הוא חוג נתר.

הוכחה: הראינו אפיון של חוג נתר כחוג שבו כל אידאל נוצר־סופית. תחום ראשי הוא חוג שבו כל אידאל נוצר על־ידי איבר יחיד, ולכן הוא בפרט תחום נתר. ■

למה 2: בחוג נתר, לכל איבר קיים פירוק לאיברים אי־פריקים.

הוכחה: יהי R חוג נתר, כלומר, לפי איפיון נוסף שהראינו, לכל אוסף לא ריק של אידאלים בו יש איבר מירבי ביחס להכלה. כלומר אידאל שאין אידאל אחר בקבוצה המכיל אותו. בפרט תכונה זו מתקיימת עבור אוסף לא ריק של אידאלים ראשיים.

תהי $Y \subset R$ קבוצת האיברים ש<u>אין</u> להם פירוק לאי־פריקים, ונראה שקבוצה זו היא $\{0\}$. נניח בשלילה שקיים $0 \neq a \in Y$. נתבונן באוסף האידאלים הראשיים של איברים ב-Y, שכאמור אינו ריק. מהיות R חוג נתר נובע שקיים $a_{\max} \in Y$ כך ש-$(a_{\max})$ אידאל ראשי מירבי ביחס להכלה.

נתבונן באיבר $a_{\max} \in Y$. אם הוא אי־פריק אז הוא מכפלה באורך 1 של אי־פריקים, בסתירה להגדרת הקבוצה Y. לכן $a_{\max}$ לא אי־פריק, כלומר קיימים $b, c \in R$ כך ש-$a_{\max} = bc$ ועדיין $a_{\max} \nsim b$ וגם $a_{\max} \nsim c$.

נשים לב שמהיות $(a_{\max})$ אידאל מירבי מבין האידאלים הראשיים של איברי Y, נובע שלכל $d \in Y$ מתקיים כי אם $(a_{\max}) \subset (d)$ אז $(a_{\max}) = (d)$. במילים אחרות: לכל $d \in Y$, אם $a_{\max} = rd$ אז $a_{\max} \sim d$. מכאן נובע בהכרח $b, c \notin Y$, ולכן יש להם פירוק לאי־פריקים. אבל $a_{\max} = bc$ ולכן גם לו יש פירוק לאי־פריקים, בסתירה להגדרת Y. ■

למה 3: בתחום ראשי כל אי־פריק הוא ראשוני.

למה 3א: אם $I \lhd R$ אידאל מירבי בתחום ראשי R, אז R/I שדה.

הוכחה: מהיות R תחום ראשי ובפרט חוג קומוטטיבי, נובע בקלות כי R/I הוא גם קומוטטיבי. נותר להראות כי R/I חוג חילוק.

נתבונן בהומומורפיזם הקנוני $h : R \to R/I$ המוגדר $h\left(r\right) = r + I$, ויהי $J \lhd R/I$ אידאל. קל לבדוק כי $h^{-1}\left(J\right) \lhd R$ אידאל וכן גם $I \subset h^{-1}\left(J\right)$. מהיות I אידאל מירבי נובע כי $h^{-1}\left(J\right) = I$ או $h^{-1}\left(J\right) = R$. מכיוון ש-h העתקה על R/I נובע כי בהתאמה $J = h\left(I\right) = I = 0_{R/I}$ או $J = h\left(R\right) = R/I$.

מכאן כי R/I חוג פשוט, ולכן לכל $a \in R/I$ מתקיים כי $R/I = 0, (a)$.
אם $(a) = \{0\}$ אז $a = 0$, ואם $(a) = R/I$ אז בפרט קיים $r \in R$ כך ש-$ar = 1$ ולכן a הפיך. ■

הוכחה: יהי $a \in R$ אי־פריק בתחום ראשי R. לכן האידאל הראשי (a) הוא מירבי בין האידאלים הראשיים.[8]

מהיות R ראשי נובע כי כל האידאלים ראשיים, ולכן האידאל (a) מירבי בין כל האידאלים באופן מוחלט, ומהלמה האחרונה נובע כי $R/(a)$ שדה.

יהי $h : R \to R/(a)$ ההומומורפיזם הקנוני ונניח כי $a|bc$. לכן קיים $d \in R$ כך ש-$ad = bc$, ולכן מהיות h הומומורפיזם נובע $h(a)\,h(d) = h(b)\,h(c)$. אבל מכיוון ש-$a \in (a)$ נובע כי $h(a) = a + (a) = (a) = 0_{R/(a)}$, ולכן $h(b) = 0$ או $h(c) = 0$. כלומר בהתאמה $b \in (a)$ או $c \in (a)$ ולכן $a|b$ או $a|c$, וזו ההגדרה לראשוניות. ■

2.6 חוג השלמים של גאוס $\mathbb{Z}[i]$

ראינו כי חוג השלמים $\mathbb{Z}$ עם הפונקציה $d(k) = |k|$ הוא חוג אוקלידי, וכן ראינו כי $\mathbb{F}[x]$ עם הפונקציה $d(f) = \deg(f)$ הוא חוג אוקלידי. נראה כעת דוגמה יסודית נוספת לחוג אוקלידי - חוג השלמים של גאוס.

הגדרה: הקבוצה $\mathbb{Z}[i] = \left\{a + bi | a, b \in \mathbb{Z},\ i^2 = -1\right\}$ עם פעולות החיבור והכפל המושרות עליו משדה המרוכבים $\mathbb{C}$, היא **חוג השלמים של גאוס**.

זהו תת־חוג של $\mathbb{C}$, שכן קל לראות כי $0, 1 \in \mathbb{Z}[i]$, וכן מתקיימת סגירות לחיבור ולכפל:

$$(a + bi) + (c + di) = (a + b) + (b + d)\,i$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (bc + ad)\,i$$

טענה: $\mathbb{Z}[i]$ עם הפונקציה $d(x) = x\overline{x}$ הוא חוג אוקלידי.[9]

מסקנה: ראינו שחוג אוקלידי הוא תחום ראשי ושבתחום ראשי קיימת פריקות חד־ערכית, ולכן ב-$\mathbb{Z}[i]$ מתקיימת פריקות חד־ערכית.

הוכחה: צריך להראות שמתקיימים שני התנאים שמגדירים חוג אוקלידי.

התנאי הראשון נובע מכך שלכל $0 \neq x \in \mathbb{Z}[i]$, לכל $0 \neq y \in \mathbb{Z}[i]$ מתקיים:

$$d(xy) = (xy)\left(\overline{xy}\right) = (x\overline{x})(y\overline{y}) = d(x)\,d(y) \geq d(x)$$

כאשר אי השוויון נובע מכך ש-$d(y)$ מספר טבעי.

כעת יש להראות את התנאי השני: לכל $x, y \in \mathbb{Z}[i]$ כאשר $y \neq 0$, קיים $s \in \mathbb{Z}[i]$ כך שמתקיים $x = ys$ או $d(x - ys) < d(y)$.

---

[8] כי אם $(b) \subset (a)$ אז $b|a$ ומאי־פריקות a נובע כי $b \sim a$ ולכן $(b) = (a)$.

[9] מגדירים $\overline{a + bi} = a - bi$. פונקציה זו היא גם הומומורפיזם.

נשים לב כי $x\bar{y} = y\bar{y}s \iff x = ys$ וכן גם בהתאמה:

$$d(x\bar{y} - y\bar{y}s) < d(y\bar{y}) \iff d(x-ys)\,d(\bar{y}) < d(y)\,d(\bar{y}) \iff d(x-ys) < d(y)$$

בגלל ש-$y\bar{y} \in \mathbb{Z}$ זו רדוקציה לבעיה של חילוק עם שארית של $x \in \mathbb{Z}[i]$ ב-$y \in \mathbb{Z}$ (במקום ב-$y \in \mathbb{Z}[i]$).

נסמן $x = u + vi$ עבור $u, v \in \mathbb{Z}$. נבחר $n, m \in \mathbb{Z}$ כאלה כך שיתקיים:

$$|r_2| = |v - my| \leq \frac{y}{2} \qquad\qquad |r_1| = |u - ny| \leq \frac{y}{2}$$

כעת נגדיר $s = n + mi$ ונראה כי $x = ys$ או $d(x-ys) < d(y)$.

מתקיים $x = u + vi = (ny + r_1) + (my + r_2)i$. אם $r_1 = r_2 = 0$ אז $x = ys$.
במקרה שלא, נחשב:

$$d(x - ys) = d(u + vi - sy) = d((ny + r_1) + (my + r_2)i - (n + mi)y) =$$

$$= d((ny + r_1 - ny) + (my + r_2 - my)i) = d(r_1 + r_2 i) = (r_1 + r_2 i)(r_1 - r_2 i) =$$

$$= r_1^2 + r_2^2 \leq \frac{y^2}{4} + \frac{y^2}{4} = \frac{y^2}{2} < y^2 = y\bar{y} = d(y)$$

■

2.6.1 ההפיכים של $\mathbb{Z}[i]$

טענה: האיברים ההפיכים ב-$\mathbb{Z}[i]$ הם $\pm 1, \pm i$ בלבד.

הוכחה: קל לראות שבאופן כללי ל-$0 \neq x + yi \in \mathbb{C}$ מתקיים כי $(x+yi)^{-1} = \frac{x-yi}{x^2+y^2}$.
מהיות $\mathbb{C}$ שדה נובע שההופכי יחיד. לכן ב-$\mathbb{Z}[i]$ כתת־חוג ב-$\mathbb{C}$, אם יש הופכי אז הוא מהצורה הנ"ל.

כעת בהינתן $a + bi \in \mathbb{Z}[i]$, קל לראות כי הביטויים $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}$ הם שלמים אם ורק אם $a = \pm 1, b = 0$ או $a = 0, b = \pm 1$.[10] מכאן שהאיברים ההפיכים ב-$\mathbb{Z}[i]$ הם רק $\pm 1, \pm i$. ■

2.6.2 הראשוניים של $\mathbb{Z}[i]$

לא כל ראשוני ב-$\mathbb{Z}$ הוא גם ראשוני ב-$\mathbb{Z}[i]$. למשל 2 ראשוני ב-$\mathbb{Z}$, אבל ב-$\mathbb{Z}[i]$ מתקיים כי $2 = (1+i)(1-i)$, וכפי שהראינו $1+i, 1-i$ אינם הפיכים ב-$\mathbb{Z}[i]$, ולכן 2 מתפרק למכפלה של שני איברים שהוא אינו חבר של שניהם, ולפיכך הוא אינו ראשוני ב-$\mathbb{Z}[i]$.

למה: יהי p ראשוני ב-$\mathbb{Z}$, אזי מתקיימת אחת משתי האפשרויות הבאות: p ראשוני ב-$\mathbb{Z}[i]$ או שהוא מתפצל $p = \pm q\bar{q}$ עבור q ראשוני ב-$\mathbb{Z}[i]$.

---

[10] ניתן לראות זאת פורמלית מכך שאם $y \in \mathbb{Z}[i]$ הפיך, אז יש $x \in \mathbb{Z}[i]$ כך ש-$xy = 1$. מכאן כי $1 = 1 \cdot \bar{1} = (xy)(\overline{xy}) = (x\bar{x})(y\bar{y})$.
כעת אם נסמן $x = a + bi \in \mathbb{Z}[i]$ אז $x\bar{x} = (a+bi)(a-bi) = a^2 + b^2 \in \mathbb{Z}$. מכאן כי אם נסמן גם $y = c + di \in \mathbb{Z}[i]$ אז $1 = (x\bar{x})(y\bar{y}) = (a^2+b^2)(c^2+d^2) \in \mathbb{Z}$.
קיבלנו פירוק של 1 לשני שלמים, ולכן בהכרח $(a^2+b^2) = \pm 1$, ומכאן כי $a = 0, b = \pm 1$ או להיפך.

דוגמאות: ראינו ש-2 אינו ראשוני ב-$\mathbb{Z}[i]$ אולם הוא מתפצל $2=(1+i)(1-i)$,
ולכן מהלמה ינבע כי $\pm(1+i),\pm(1-i)$ ראשוניים ב-$\mathbb{Z}[i]$.

מתקיים גם $q\overline{q}\neq 3$ לכל $q\in\mathbb{Z}[i]$, כי אם נסמן $q=n+mi$ אז $q\overline{q}=n^2+m^2$.
אבל 3 אינו סכום של אף שני ריבועים שלמים, ולכן מהלמה הוא ראשוני ב-$\mathbb{Z}[i]$.

הוכחה: יהי p ראשוני ב-$\mathbb{Z}$. מכיוון ש-$\mathbb{Z}[i]$ תחום פריקות חד־ערכית, נסמן את הפירוק של p לראשוניים $p=q_1\cdot\ldots\cdot q_n$ ל-$1\leq n$, כאשר $q_i\in\mathbb{Z}[i]$.

נשים לב כי מקומוטטיביות החוג ומכך ש-p שלם נובע:

$$p^2=p\overline{p}=q_1\cdot\ldots\cdot q_n\overline{q_1}\cdot\ldots\cdot\overline{q_n}=q_1\overline{q_1}\cdot\ldots\cdot q_n\overline{q_n}$$

בפרט מתקיים כי $\mathbb{Z}\ni q_1\overline{q_1}>0$ וכן $q_1\overline{q_1}|p^2$. אבל מהיות p ראשוני נובע כי שבהכרח $q_1\overline{q_1}\in\{1,p,p^2\}$.

לא ייתכן $q_1\overline{q_1}=1$ כי q_1 לא הפיך. לכן $q_1\overline{q_1}=p$ או $q_1\overline{q_1}=p^2$.

אם $q_1\overline{q_1}=p$ קיבלנו את האפשרות השנייה בלמה. אם $q_1\overline{q_1}=p^2$ אז $p^2=q_1\overline{q_1}\cdot\ldots\cdot q_n\overline{q_n}$. קיבלנו שני פירוקים של p^2 כמכפלה של ראשוניים, ולכן אורך הפירוקים שווה. כלומר $2n=2$ ולכן $n=1$. כלומר, אם נחזור לפירוק של p נקבל $p=q_1$, וקיבלנו את האפשרות הראשונה בלמה. ■

למה: יהי p ראשוני ב-$\mathbb{Z}$ (נניח ללא הגבלת הכלליות שהוא חיובי), אזי התנאים הבאים שקולים:

1. p <u>איננו</u> ראשוני ב-$\mathbb{Z}[i]$.
2. $p=q\overline{q}$. כלומר p הוא סכום של שני ריבועים ב-$\mathbb{Z}$.
3. בשדה הסופי $\mathbb{F}_p\cong\mathbb{Z}/p\mathbb{Z}$ קיים $\sqrt{-1}$. כלומר קיים $x\in\mathbb{F}_p$ כך ש-$x^2=-1$.
4. $4|p-1$. כלומר $p\equiv 1 \mod (4)$.

הוכחה:

- $(1\Longleftarrow 2)$ אם p איננו ראשוני ב-$\mathbb{Z}[i]$, מהלמה הקודמת נובע שהוא מתפצל. כלומר $p=(m+ni)(m-ni)=m^2+n^2$.
- $(2\Longleftarrow 3)$ נניח כי $p=m^2+n^2$. לכן בפרט $m,n<p$ ומכאן $m,n\not\equiv 0 \mod (p)$.

  נסמן $\overline{m}\equiv m \mod (p)$, $\overline{n}\equiv n \mod (p)$, ונסיק כי:

$$m^2+n^2=p\implies \overline{m}^2+\overline{n}^2=0\implies\overline{m}^2=-\overline{n}^2\implies\left(\frac{\overline{m}}{\overline{n}}\right)^2=-1$$

- $(3\Longleftarrow 1)$ נניח כי $\overline{m}\in\mathbb{F}_p$ מקיים $\overline{m}^2=-1$. נתבונן במספר m כמספר ב-$\mathbb{Z}$ ונסיק כי:

$$\mathbb{N}\ni m^2+1\equiv 0 \mod (p)\implies p|m^2+1=(m+i)(m-i)$$

  אבל $p\nmid m+i,m-i$ כי אם $p\cdot(a+bi)=pa+pbi=m+i$ אז $m\equiv 0 \mod (p)$, וזו סתירה כי $m^2\equiv -1 \mod (p)$.

  מכאן כי p אינו אי־פריק, ולכן הוא לא ראשוני.

- (3 $\Longleftrightarrow$ 4) נשים לב שבחבורה הכפלית $\mathbb{Z}_p^*$, קיום איבר מסדר 4, כלומר $y^4=1$ כך ש-4 מינימלי ביחס לתכונה זו, שקול לכך שיתקיים $y^2=-1$.[11]
  כעת נשים לב שקיום איבר מסדר 4 בחבורה $\mathbb{Z}_p^*$ שקול לכך שקיימת תת־חבורה מגודל 4 הנוצרת על־ידו. ממשפט לגראנז' נובע $4\left|\left|\mathbb{Z}_p^*\right|=p-1\right.$. ■

הערה: ניתוח דומה לזה שעשינו לחוג השלמים של גאוס $\mathbb{Z}[i]$ ניתן לבצע לחוג הקווטרניונים, שהוא אינו קומוטטיבי.[12]

3 חוגי פולינומים

הגדרה: אם R חוג קומוטטיבי, אז $R[x]$ הוא חוג הפולינומים במשתנה אחד מעליו.

איבר כלשהו ב-$R[x]$ הוא מהצורה $f(x)=a_nx^n+...+a_1x+a_0$, כאשר $a_i\in R$, $1\le i\le n$.

בהנחה ש-$a_n\neq 0$ מגדירים ומסמנים את דרגת הפולינום להיות $\deg(f)=n$.

חיבור וכפל בחוג זה מוגדרים סטנדרטית, לפי הכלל $x^k\cdot x^l=x^{k+l}$ ל-$k,l\in\mathbb{Z}$.

מהיות R חוג קומוטטיבי נובע בקלות כי $R[x]$ חוג קומוטטיבי.

הערה: באופן כללי מתקיים כי $\deg(f\cdot g)\le\deg(f)+\deg(g)$, ואם R תחום שלמות אז מתקיים שוויון ממש.[13]

הערה: ניתן להגדיר את חוג הפולינומים בשני משתנים על־ידי $R[x,y]=R[x][y]$.

כלומר $R[x]$ הוא חוג, ולכן ניתן לדבר על פולינומים במשתנה אחד מעליו. דהיינו פולינומים שהמשתנה שלהם הוא פולינום.

אינדוקטיבית ניתן להגדיר כך חוג פולינומים בכל מספר סופי של משתנים.

רקע: נדון בתחום פריקות חד־ערכית R ובשדה השברים שלו K. הדיון יהיה אנלוגי לחוג $\mathbb{Z}$ ולשדה השברים שלו $\mathbb{Q}$.

1. נזכור כי p ראשוני אם ורק אם $R/(p)$ תחום שלמות.
2. לכל מספר סופי של איברים בחוג R קיים מחלק משותף מקסימלי (gcd).
   כלומר אם $a_1,...,a_n\in R$, אז קיים $b\in R$ כך שמתקיים $b|a_i$ לכל $1\le i\le n$ והוא מקסימלי ביחס לתכונה זו. כלומר לכל $b'\in R$ שגם מקיים $b'|a_i$ לכל $1\le i\le n$, מתקיים כי $b'|b$.

   הערה: נשים לב כי b אינו בהכרח יחיד כי הוא מוגדר עד־כדי חברות, ולכן את הסימון $\gcd(a_1,...,a_n)=b$ צריך לקחת בעירבון מוגבל.

---

[11] ברור שאם $y^2=-1$ אז $y^4=1$, ומצד שני לא ייתכן $y^2=1$ ממינימליות 4, ולכן בהכרח $y^2=-1$.

[12] חוג הקווטרניונים הוא החוג $\mathbb{R}[i,j,k]$, כאשר i,j,k כולם שורשי מינוס יחידה וכן $ijk=-1$.

דרך יעילה להסתכל על חוג הקווטרניונים היא $\begin{matrix} & i & \\ k & & j\end{matrix}$, כאשר מכפלת כל שניים עוקבים בכיוון השעון נותנת את האיבר הבא, ומכפלת כל שניים עוקבים נגד כיוון השעון נותנת את מינוס האיבר הבא.

[13] במקרה ש-R אינו תחום שלמות ייתכן למשל עבור $f(x)=a_nx^n$, $g(x)=b_mx^m$ שיתקיים $a_n,b_m\neq 0$ אבל $a_n\cdot b_m=0$.

הוכחה: נוכיח קיום של gcd על־ידי בנייה מפורשת שלו. תהי $\mathcal{P}$ קבוצת הראשוניים של R המכילה נציג אחד מכל מחלקת חברות.[14]

יהיו $a_1,...,a_n \in R$. כל a_i ניתן לפרק $a_i = u \cdot p_1^{m_1} \cdot ... \cdot p_j^{m_j}$ ל-$0 \leq m_i$, כאשר u הפיך וכן $p_i \in \mathcal{P}$.

יהיו $p_1,...,p_l \in \mathcal{P}$ קבוצת כל הראשוניים שמופיעים בפירוק כלשהו של $a_1,...,a_n$. כלומר לכל $1 \leq i \leq n$ מתקיים $a_i = u_i p_1^{m_{i1}} \cdot ... \cdot p_l^{m_{il}}$ כאשר $0 \leq m_i$.

כעת לכל i נגדיר:

$$j_1 = \min\{m_{11},...,m_{n1}\}$$
$$\vdots$$
$$j_l = \min\{m_{1l},...,m_{nl}\}$$

וכעת נגדיר $b = p_1^{j_1} \cdot ... \cdot p_l^{j_l}$ ונקבל כי b הוא $\gcd(a_1,...,a_n)$. ■

הערה: בתחום ראשי מתקיים כי $\gcd(a_1,a_2) \in (a_1,a_2)$ (כלומר האידאל הנוצר), מהלמה של בזו.
אך למשל ב-$\mathbb{Z}[x]$ זה לא נכון. מצד אחד $\gcd(2,x)=1$ אבל $1 \notin (2,x)$.

3.1 הלמה של גאוס

משפט: אם p ראשוני ב-R, אז הוא גם ראשוני ב-$R[x]$. כלומר אם $p|fg$ אזי $p|f$ או $p|g$.

הערה: המשמעות של $p|f$ היא שאם $f = a_n x^n + ... + a_1 x + a_0$, אז קיים פולינום $g = b_n x^n + ... + b_1 x + b_0$ כך ש-$pg = f$, כלומר $pb_j = a_j$ לכל $1 \leq j \leq n$.

הוכחה: נסמן $\overline{R} = {}^{R}/_{(p)}$. מהיות p ראשוני נובע כי $\overline{R}$ תחום שלמות. מכאן שגם $\overline{R}[x]$ תחום שלמות.

נתבונן בהומומורפיזם $\varphi : R \to \overline{R}$ המוגדר על־ידי $x \mapsto \overline{x} =: x + (p)$. ניתן לראות שהומומורפיזם זה ניתן להרחבה להומומורפיזם $R[x] \to \overline{R}[x]$ כאשר הפעולה היא על המקדמים של f.

מההנחה $p|fg$ נובע כי $fg \in (p)$ ולכן $\overline{f} \cdot \overline{g} = \overline{0}$. מהיות $R[x]$ תחום שלמות נסיק כי $\overline{f} = \overline{0}$ או $\overline{g} = \overline{0}$. נניח ללא הגבלת הכלליות כי $\overline{g} = \overline{0}$ ונסמן $g = \sum a_i x^i$, משמע לכל i מתקיים $\overline{a_i} = 0$ כלומר $a_i \in (p)$ ולכן $p|a_i$. מכאן כי $p|g$. ■

הגדרה: פולינום $f \in R[x]$ נקרא **פרימיטיבי**, אם אין ראשוני $p \in R$ שמחלק אותו. כלומר אין ראשוני p המחלק את כל מקדמי f, משמע ה-gcd של מקדמי f הוא 1.

את אוסף הפולינומים הפרימיטיביים ב-$R[x]$ נסמן $R[x]_{prim}$.

הלמה של גאוס: (גרסה 1) אם f,g פרימיטיביים אז גם fg פרימיטיבי.

הוכחה: נניח בשלילה כי fg אינו פרימיטיבי, ולכן קיים p ראשוני ב-R המקיים $p|fg$.

מהמשפט שהוכחנו נובע כי p ראשוני גם ב-$R[x]$, ולכן בהכרח $p|f$ או $p|g$, בסתירה להיות f,g פרימיטיביים. ■

הגדרה: בהינתן $f = \sum_{i=1}^{n} a_i x^i \in R[x]$, קיים $c = \gcd(a_0,...,a_n)$. ל-c הנ"ל קוראים **התוכן** של הפולינום f.

[14] האנלוגיה ל-$\mathbb{Z}$ היא שלוקחים למשל רק את הראשוניים החיוביים.

טענה: לכל $f \in K[x]$,[15] קיימים $c \in K$ ו-$g \in R[x]_{prim}$ כך ש-$f = cg$.

הוכחה: נטפל תחילה במקרה $f \in R[x]$. הראינו שקיים תוכן c, ולכן מוגדר היטב הפולינום $g = \frac{a_0}{c} + \frac{a_1}{c}x + ... + \frac{a_n}{c}x^n$, כי $c = \gcd(a_0, ..., a_n)$ ולכן $\frac{a_j}{c} \in R$ לכל $1 \leq j \leq n$.

נשים לב כי g פרימיטיבי, כי אם היה ראשוני שמחלק את כל מקדמי g, אז c היה מחלק משותף לא מקסימלי. מכאן הטענה נובעת עבור $R[x]$.

כעת בהינתן $f = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + ... + \frac{a_n}{b_n}x^n \in K[x]$, עבור $b = b_0 \cdot b_1 \cdot ... \cdot b_n$ (המכנה המשותף) מתקיים $bf \in R[x]$.

לפולינומים ב-$R[x]$ קיים תוכן c ו-$g \in R[x]_{prim}$ כך שמתקיים $bf = cg$, ולכן $f = \frac{c}{b}g$ ל-$\frac{c}{b} \in K$. ■

טענה: לכל פולינום ב-$K[x]$ התוכן מוגדר היטב עד־כדי חברות ב-R.

הוכחה: יהי $f \in K[x]$ ונניח כי c_1, c_2 תוכנים שלו. נטפל תחילה במקרה $c_1, c_2 \in R$.

כפי שהראינו קיימים פולינומים $g_1, g_2 \in R[x]_{prim}$ כך שמתקיים $f = c_1g_1$ וגם $f = c_2g_2$.

מהיות g_1 פרימיטיבי נובע כי c_1 הוא ה-gcd של מקדמי הפולינום c_1g_1, אבל $c_1g_1 = c_2g_2$ ולכן c_1 הוא ה-gcd של מקדמי הפולינום c_2g_2.

מצד שני מהיות g_2 פרימיטיבי נובע כי c_2 הוא ה-gcd של מקדמי הפולינום c_2g_2, ולכן c_1, c_2 שניהם gcd של אותה קבוצת איברים ב-R. כפי שהזכרנו לעיל gcd מוגדר היטב עד־כדי חברות, ולכן בהכרח c_1, c_2 חברים.

כעת נטפל במקרה $c_1, c_2 \in K$. הראינו שקיים $b \in R$ כך ש-$bc_1g_1 = bc_2g_2 \in R[x]$ (המכנה המשותף), ולכן מאותו נימוק bc_1, bc_2 חברים ב-R. כלומר יש $u \in R$ הפיך כך ש-$bc_1 = bc_2u$ ונקבל כי $c_1 = c_2u$, כלומר הם חברים ב-R. ■

הגדרה: נגדיר את U להיות אוסף האיברים ההפיכים ב-R. נגדיר העתקה $\underline{c} : K[x]^* \to {K^*}/{U}$ על־ידי $\underline{c}(f) = cU$, כלומר כל $f \in K[x]^*$ מועתק ל-cU, כאשר c התוכן של f, כלומר הקבוע המקיים $f = cg$ ל-$g \in R[x]_{prim}$.

הערה: הראינו שהתוכן c של f מוגדר היטב עד־כדי חברות, ולכן אם c_1, c_2 תוכנים של f אז $c_1U = c_2U$ כי הם חברים. לכן ההעתקה $\underline{c}$ מוגדרת היטב מודולו ההפיכים U.

הלמה של גאוס: (גרסה 2) $\underline{c}(fg) = \underline{c}(f)\underline{c}(g)$

הוכחה: יהיו $f, g \in K[x]$ ונניח שהתוכנים המתאימים הם $c, d \in K$, כך שמתקיים $f = cf_1$, $g = dg_1$, עבור $g_1, f_1 \in R[x]_{prim}$.

לכן מתקיים $fg = cdf_1g_1$. אבל f_1, g_1 פרימיטיביים ולכן כפי שהוכחנו לעיל נובע כי f_1g_1 פרימיטיבי, ומכאן כי $\underline{c}(f_1g_1) = U$ (כלומר $\underline{c}(f_1g_1) = 1$ בחוג המנה ${K^*}/{U}$), ולכן:

$$\underline{c}(cdf_1g_1) = cdU = cUdU = \underline{c}(f)\underline{c}(g)$$

■

[15] K הוא שדה השברים של R.

טענה: יהיו $f\in R\left[x\right]_{prim}$, $g\in R\left[x\right]$. אזי $f|g$ ב-$R\left[x\right]$ אם ורק אם $f|g$ ב-$K\left[x\right]$.

הוכחה: ברור שאם $f|g$ ב-$R\left[x\right]$ אז בפרט $f|g$ ב-$K\left[x\right]$. נראה את הכיוון השני.

נניח כי $g=hf$ ל-$h\in K\left[x\right]$. מהלמה של גאוס נובע $\underline{c}\left(g\right)=\underline{c}\left(hf\right)=\underline{c}\left(h\right)\underline{c}\left(f\right)=\underline{c}\left(h\right)$, שכן f פרימיטיבי ולכן $\underline{c}\left(f\right)=1$. אבל $g\in R\left[x\right]$ ולכן $\underline{c}\left(g\right)\in R$, ומהשוויון הנ"ל נובע שגם $\underline{c}\left(h\right)\in R$.

נציג את h באמצעות $h=\underline{c}\left(h\right)h_1u$ ל-$h_1\in R\left[x\right]$ (כפי שהראינו לעיל), ונסיק כי $h\in R\left[x\right]$, כי הוא מכפלה של סקלר ב-R עם פולינום $h_1\in R\left[x\right]$. כלומר השוויון $g=hf$ הוא למעשה שוויון ב-$R\left[x\right]$ ולכן $f|g$ ב-$R\left[x\right]$. ■

מסקנה: אם $f\in R\left[x\right]_{prim}$ אי־פריק ב-$K\left[x\right]$, אז f ראשוני ב-$R\left[x\right]$.

הערה: $K\left[x\right]$ הוא תחום ראשי ולכן אי־פריק זה ראשוני. לעומת זאת $R\left[x\right]$ אינו בהכרח כזה, ולכן f לא בהכרח אי־פריק ב-$R\left[x\right]$.

הוכחה: נניח כי $f|gh$ ל-$g,h\in R\left[x\right]$, לכן בפרט הוא גם מחלק אותם ב-$K\left[x\right]$. מהיות f אי־פריק ב-$K\left[x\right]$ נובע כי $f|g$ או $f|h$ ב-$K\left[x\right]$.

מהטענה האחרונה נובע כי גם $f|g$ או $f|h$ ב-$R\left[x\right]$, כלומר f ראשוני ב-$R\left[x\right]$. ■

טענה: כל פולינום אי־פריק ב-$R\left[x\right]$, הוא אי־פריק ב-$K\left[x\right]$.

הוכחה: יהי $f\in R\left[x\right]$ אי־פריק ב-$R\left[x\right]$. נניח $f=gh$ ל-$g,h\in K\left[x\right]$. נראה כי g הפיך או h הפיך.[16]

נכתוב $g=c_1\tilde{g}$, $h=c_2\tilde{h}$ ל-$\tilde{g},\tilde{h}\in R\left[x\right]_{prim}$ עבור $c_1,c_2\in K$. נגדיר $c=c_1\cdot c_2\in K$ ונסמן $c=\frac{a}{b}$ ל-$a,b\in R$ זרים.

בסימונים אלה נקבל $f=gh=c_1\tilde{g}c_2\tilde{h}=\frac{a}{b}\tilde{g}\tilde{h}$. אם נראה כי $\frac{a}{b}\in R$ נסיים, כי מאי־פריקות f מעל $R\left[x\right]$ ינבע כי שבהכרח $\tilde{g}$ הפיך או $\tilde{h}$ הפיך.

אבל מפרימיטיביות $\tilde{g},\tilde{h}$ נובע כי b לא יצטמצם עם כפולה שלהם, ומכאן $bf=a\tilde{g}\tilde{h}$. מהלמה של גאוס נובע כי מפרימיטיביות $\tilde{g},\tilde{h}$ גם $\tilde{g}\tilde{h}$ פרימיטיבי, ולכן אם נתבונן בפירוק הכללי $f=c\left(f\right)\tilde{f}$, נסיק מהשוויון האחרון כי $bc\left(f\right)=a$. אבל a,b זרים ולכן בהכרח b הפיך ב-R. מכאן כי $\frac{a}{b}\in R$. ■

משפט: אם R תחום פח"ע אז גם $R\left[x\right]$ תחום פח"ע.

הוכחה: יהי $f\in R\left[x\right]$. בפרט $f\in K\left[x\right]$ ו-$K\left[x\right]$ חוג אוקלידי כי K שדה, ולכן תחום ראשי ולכן תחום פח"ע. לכן $f=v\cdot f_1\cdot\ldots\cdot f_n$ עבור $f_1,...,f_n\in K\left[x\right]$ ראשוניים ול-$v\in K$ הפיך.

ניתן להכפיל במכנה משותף של כל $f_1,...,f_n$ כך שכולם ב-$R\left[x\right]$, לכן נניח ללא הגבלת הכלליות כי $f_1,...,f_n\in R\left[x\right]$.

כפי שראינו ניתן לבטא $f_i=c_ig_i$ ל-$g_i\in R\left[x\right]_{prim}$ ו-$c_i\in R$, ולכן נקבל $f=v\cdot c_1\cdot\ldots\cdot c_n\cdot g_1\cdot\ldots\cdot g_n$. נראה שפירוק זה ייתן פירוק לראשוניים של $R\left[x\right]$.

- $g_1,...,g_n$ ראשוניים של $R\left[x\right]$, כי הראינו במסקנה לעיל שאיבר של $R\left[x\right]_{prim}$ שהוא ראשוני של $K\left[x\right]$ הוא גם ראשוני של $R\left[x\right]$.

[16] בהתאם לאיפיון שקול לאי־פריקות שהראינו לעיל.

• כעת מספיק להראות $v \cdot c_1 \cdot ... \cdot c_n \in R$ ונסיים. נשים לב שמתקיים:

$$c(f) = c(v \cdot c_1 \cdot ... \cdot c_n \cdot g_1 \cdot ... \cdot g_n) = c(v \cdot c_1 \cdot ... \cdot c_n) \cdot \underbrace{c(g_1 \cdot ... \cdot g_n)}_{=1} \cdot u =$$

$$= c(v \cdot c_1 \cdot ... \cdot c_n) \cdot u = v \cdot c_1 \cdot ... \cdot c_n \cdot u$$

ל-$u \in R$ הפיך כלשהו. כאשר השוויון השני נובע מהלמה של גאוס, השוויון השלישי מכך שכל g_i פרימיטיבי, והשוויון הרביעי מכך ש-$v \cdot c_1 \cdot ... \cdot c_n$ סקלר. אבל $f \in R[x]$ ולכן $c(f) \in R$ ומכאן $v \cdot c_1 \cdot ... \cdot c_n \cdot u \in R$. ■

3.2 הקריטריון של אייזנשטיין

רקע: נרצה דרך לדעת האם פולינום של $\mathbb{Q}[x]$ הוא אי־פריק. קל לראות שהכפלה במכנה המשותף של המקדמים שב-$\mathbb{Q}$ תיתן לנו פולינום ב-$\mathbb{Z}[x]$.

לעיל הוכחנו שפולינום אי־פריק ב-$R[x]$ הוא גם אי־פריק ב-$K[x]$, ולכן קיבלנו רדוקציה של הבעיה לפריקות ב-$\mathbb{Z}[x]$.

נתמודד עם בעיה זו באמצעות הומומורפיזמים: בהינתן $f \in \mathbb{Z}[x]$, נתבונן בהומומורפיזם $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ל-n כלשהו, המוגדר $f \mapsto \overline{f}$ (כלומר לוקחים כל מקדם $\mod (n)$).

נשים לב שאם f מתפרק $f = g \cdot h$, אז $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h}$ (כי זה הומומורפיזם). לכן נראה שתחת תנאים מסוימים, כדי לדעת ש-f אי־פריק מעל $\mathbb{Z}$ די לדעת שהוא אי־פריק מעל $\mathbb{Z}/n\mathbb{Z}$ ל-n כלשהו.

הקריטריון: יהי $f(x) = a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x]$. אם קיים p ראשוני כך שמתקיים:

1. $p | a_0, ..., a_{n-1}$
2. $p \nmid a_n$
3. $p^2 \nmid a_0$

אזי f אי־פריק מעל $\mathbb{Z}[x]$, ולכן גם אי־פריק מעל $\mathbb{Q}[x]$.

הוכחה: נסמן $\overline{f} = f \mod (p)$. מההנחות נובע כי $\overline{f} = \overline{a}_n x^n$. נניח בשלילה כי $f = gh$ עבור $1 \leq \deg(g), \deg(h)$. לכן $\overline{a}_n x^n = \overline{g}\overline{h}$ ומהיות $\mathbb{F}_p[x]$ תחום פריקות יחידה ניתן לסמן $\overline{a}_n = de$ ל-$d, e \in \mathbb{Z}/p\mathbb{Z}$ המקיימים $\overline{g} = dx^m,\ \overline{h} = ex^{n-m}$.

מכאן שכל מקדמי g, h האחרים הם $0 \mod (p)$, ובפרט גם המקדמים החופשיים. אבל מכפלת המקדמים החופשיים של g, h היא המקדם החופשי של f, ולכן קיבלנו סתירה להנחה 3. ■

דוגמה יסודית: נבחן את הפריקות של הפולינום $x^p - 1$ ל-$p \in \mathbb{Z}$ ראשוני כלשהו.[17] קל לראות שניתן לפרק:[18]

$$x^p - 1 = (x-1)\left(x^{p-1} + ... + x + 1\right)$$

אפשר להשתמש בקריטריון אייזנשטיין כדי להראות שלא ניתן לפרק פולינום זה יותר מכך. כלומר שהפולינום $x^{p-1} + ... + x + 1$ אי־פריק.[19]

[17] מהלמה של גאוס נובע שאין הבדל בין אם נבחן את הפולינום הזה מעל $\mathbb{Z}[x]$ או מעל $\mathbb{Q}[x]$.
[18] זה הסכום הטלסקופי שנותן את נוסחת הטור ההנדסי.
[19] רמז: כדאי להתבונן בפולינום $f(x) = x^{p-1} + ... + x + 1$ עם ההצבה $x = y + 1$, ולהשתמש בנוסחת הבינום.

הערה: ניתן היה לחשוב שהפולינום $x^{p-1}+...+x+1$ הוא אי־פריק $\mod (p)$ ומכך להסיק את אי הפריקות שלו ב-$\mathbb{Z}[x]$, אולם ההפך הוא הנכון; הפולינום הזה פריק לחלוטין $\mod (p)$.

נראה כי $x^p-1=(x-1)^p \mod (p)$, ומכך נסיק $\left(x^{p-1}+...+x+1\right)=(x-1)^{p-1} \mod (p)$.

טענה: (הכללה של הטענה $x^p-1=(x-1)^p$) יהי R חוג קומוטטיבי שבו $p=0$.[20] אזי ההעתקה $x\mapsto x^p$ היא הומומורפיזם של חוגים $R\to R$ ("**הומומורפיזם פרוביניוס**").

הוכחה: קל לראות כי $0\mapsto 0$, $1\mapsto 1$ וכן $xy\mapsto x^py^p$. נוכיח את החיבוריות לפי נוסחת הבינום:

$$(x+y)^p=x^p+\binom{p}{1}x^{p-1}y+...+\binom{p}{p-1}xy^{p-1}+y^p$$

אבל לכל $1\le k<p$ מתקיים $\binom{p}{k}=\frac{p!}{k!(p-k)!}=0 \mod (p)$, כי שני הגורמים במכנה הם מכפלת איברים קטנים ממש מ-p. מכאן כי $x+y\mapsto (x+y)^p\equiv x^p+y^p \mod (p)$. ■

4 משפט המבנה למודולים נוצרים־סופית

משפט: כל חבורה אבלית נוצרת־סופית איזומורפית לסכום ישר - לא יחיד - של חבורות ציקליות, מהצורה $\mathbb{Z}/n_1\mathbb{Z}\times...\times\mathbb{Z}/n_l\mathbb{Z}\times\mathbb{Z}^k$ ל-$n_1,...,n_l\in\mathbb{Z}$.[21]

משפט: (הכללה של המשפט הקודם) יהי R חוג אוקלידי כל R־מודול נוצר־סופית איזומורפי לסכום ישר - לא יחיד - של מודולים ציקליים.[22]

הערה: המשפט הקודם מתקבל על ידי לקיחת $R=\mathbb{Z}$, והתובנה שכל חבורה אבלית היא מודול מעל השלמים.[23]

נוסח שקול: יהי R חוג אוקלידי ויהי A R־מודול נוצר־סופית, אזי קיימים $a_1,...,a_n\in A$ כך שמתקיים:

1. כל איבר של A הוא מהצורה $r_1a_1+...+r_na_n$ ל-$r_1,...,r_n\in R$ מתאימים.[24]
2. $a_1,...,a_n$ הם **כמעט חופשיים**. כלומר: אם $r_1a_1+...+r_na_n=0$, אזי $r_ia_i=0$ לכל $1\le i\le n$.[25]

הערה: המשפט תקף לכל חוג ראשי, אולם אנו נעסוק בחוגים אוקלידיים.

הגדרה: בהינתן קבוצת יוצרים $a_1,...,a_n$ ל-R־מודול A, אומרים כי $r_1,...,r_n\in R$ שלא כולם 0 הם **יחס** על $a_1,...,a_n$, אם $r_1a_1+...+r_na_n=0$.

---

[20] למשל $\mathbb{F}_p$ או $\mathbb{F}_p[x]$.

[21] נשים לב שלא דרשנו ש-$n_1,...,n_l$ יהיו זרים בזוגות, כלומר ייתכנו חזרות.

[22] מודול ציקלי הוא מודול מהצורה aR ל-$a\in R$.

[23] על ידי ההומומורפיזם $\mathbb{Z}\times A\to A$ המוגדר $(n,a)\mapsto \underbrace{a+...+a}_{n\,\text{times}}$.

[24] טענה זו היא תרגום מידי של ההנחה ש-A נוצר־סופית.

[25] בבסיס למרחב ווקטורי מעל שדה במקרה כזה היה $r_i=0$ לכל $1\le i\le n$, אולם כאן מחלישים את הדרישה.

הוכחה: הטענה הראשונה היא תרגום של ההנחה ש-A הוא R־מודול נוצר־סופית. נראה שיש יוצרים כמעט חופשיים.

במקרה שבו לאף קבוצת יוצרים אין כלל יחס, הטענה השנייה מידית. לכן נניח שקיימת קבוצת יוצרים עם יחס כלשהו עליה, ונוכיח את הטענה השנייה באינדוקציה על n.

נתבונן באוסף כל קבוצות היוצרים של A וניקח את אוסף כל היחסים האפשריים עליהן. קיים r כך ש-$d\left(r\right)$ הוא מינימלי, שכן זו קבוצה לא ריקה של טבעיים. לפיכך נניח כי $a_1,...,a_n$ היא קבוצת יוצרים עם יחס $r_1,...,r_n$ עליה, כך שללא הגבלת הכלליות $r_1 \neq 0$ ומקיים כי $d\left(r_1\right)$ מינימלי גלובלית.

למה: בסימונים לעיל מתקיים:

1. $r_1 | r_k$ לכל k.
2. לכל יחס אחר $r'_1,...,r'_n$ על קבוצת יוצרים זו מתקיים גם $r_1 | r'_k$ לכל k.

הוכחת הלמה:

1. נניח בשלילה שללא הגבלת הכלליות $r_1 \nmid r_2$. מאוקלידיות החוג R נובע שאם נחלק את r_2 ב-r_1 עם שארית קיים $s \in R$ כך ש-$d\left(r_1\right) > d\left(r_2 - sr_1\right)$.

   נשים לב כי $a_1 + sa_2, a_2, a_3, ..., a_n$ גם היא קבוצת יוצרים.[26] עוד נשים לב שהקבוצה $r_1, r_2 - sr_1, ..., r_n$ היא יחס על קבוצת יוצרים חדשה זו. אבל בחרנו את r_1 להיות בעל דרגה מינימלית גלובלית, ולכן בהכרח $d\left(r_1\right) \leq d\left(r_2 - sr_1\right)$, סתירה. לכן החלוקה היא ללא שארית, כלומר $r_1 | r_2$.

2. יהי יחס $r'_1 a_1 + ... + r'_n a_n = r_1 a_1 + ... + r_n a_n = 0$. נראה ללא הגבלת הכלליות כי $r_1 | r'_1$.

   מהיות R חוג אוקלידי ובפרט תחום ראשי נובע שמוגדר $g =: \gcd\left(r_1, r'_1\right)$, ומהלמה של בזו קיימים s_1, s'_1 כך שמתקיים $g = s_1 r_1 + s'_1 r'_1$. נסיק:

$$s_1\left(\sum_{i=1}^{n} r_i a_i\right) + s'_1\left(\sum_{i=1}^{n} r'_i a_i\right) = 0$$
$$\Downarrow$$
$$\sum_{i=1}^{n}\left(s_1 r_i + s'_1 r'_i\right) a_i = 0$$
$$\Downarrow$$
$$g a_1 + \sum_{i=2}^{n}\left(s_1 r_i + s'_1 r'_i\right) a_i = 0$$

   לכן קיבלנו יחס חדש כלשהו על $a_1,...,a_n$, וממזעריות $d\left(r_1\right)$ נסיק $d\left(r_1\right) \leq d\left(g\right)$.

   כעת נשים לב כי $r_1 = bg$ ל-$b \in R$ כלשהו, ולכן מתכונת החוג האוקלידי נקבל $d\left(g\right) \leq d\left(bg\right) = d\left(r_1\right)$. מכאן $d\left(r_1\right) = d\left(g\right)$ ולכן $g \sim r_1$ ביחס החברות.[27] אבל מתקיים $g | r'_1 \sim r_1$ ולכן $r_1 | r'_1$. ■

---

[26] מכיוון שכל אחד מאיברי קבוצת היוצרים המקורית מתקבל כקומבינציה לינארית של קבוצה זו.

[27]

הערה: קל לראות שבחוג אוקלידי, לכל אידאל aR הדרגה $d\left(a\right)$ היא מינימלית מבין דרגות איברי האידאל.

למה: יהיו $x, y \in R$ ל-R אוקלידי. אם $x | y$ וגם $d\left(x\right) = d\left(y\right)$ אז $x \sim y$ ביחס החברות.

הוכחה: קל לראות כי $x \sim y$ ביחס החברות אם ורק אם האידאלים הראשיים שלהם שווים. נוכיח כי $xR = yR$.
מהנתון $x | y$ נובע $y = xa$ ל-$a \in R$ כלשהו, ולכן $xaR \subseteq xR$. נוכיח $xR \subset xaR$.
יהי $xs \in xR$, נחלק את xs ב-xa עם שארית ונקבל $xs = xac + r$. אם בשלילה $r \neq 0$ כך ש-$d\left(xs - xac\right) < d\left(xa\right) = d\left(x\right)$, נקבל ש-$xs - xac \in xR$ הוא בעל דרגה קטנה מדרגת x. אבל דרגת x היא המינימלית באידאל xR, וזו סתירה. לכן $r = 0$ ומכאן $xs = xac \in xaR$, כלומר $xR \subset xaR$. ■

אם כך בהינתן $r_1a_1 + ... + r_na_n = 0$ ראינו כי $r_1|r_j$ לכל $2 \leq j \leq n$, ולכן נכתוב $r_1\left(a_1 + s_2a_2 + ... + s_na_n\right) = 0$.

נסמן $\hat{a}_1 =: a_1 + s_2a_2 + ... + s_na_n$ ונתבונן בקבוצת היוצרים החדשה $\hat{a}_1, a_2, ..., a_n$ שעבורה $r_1\hat{a}_1 = 0$.

כעת נתבונן במודול A' הנוצר על־ידי $a_2, ..., a_n$. מהנחת האינדוקציה קיימת קבוצת יוצרים $\tilde{a}_2, ..., \tilde{a}_n$ כפי שנדרש במשפט.

טענה: הקבוצה $\hat{a}_1, \tilde{a}_2, ..., \tilde{a}_n$ היוצרת את המודול A מקיימת גם את טענה 2 במשפט.

הוכחה: נניח כי $t_1\hat{a}_1 + t_2\tilde{a}_2 + ... + t_n\tilde{a}_n = 0$. בהעברת אגפים ניכר כי $t_1\hat{a}_1 \in A'$ ולכן קיימים $t'_2, ..., t'_n$ כך ש-$t_1\hat{a}_1 = t'_2a_2 + ... + t'_na_n$.

לכן קיבלנו כי $t_1, -t'_2, ..., -t'_n$ הוא יחס חדש על קבוצת היוצרים $\hat{a}_1, a_2, ..., a_n$, ולפי חלק 2 בלמה שהראינו נובע כי $r_1|t_1$. לכן מהנתון $r_1\hat{a}_1 = 0$ נובע גם $t_1\hat{a}_1 = 0$.

כמו כן מהנחת האינדוקציה עבור כל $2 \leq j \leq n$ מתקיים כי $r_j\tilde{a}_j = 0$, ולכן קיבלנו כי $\hat{a}_1, \tilde{a}_2, ..., \tilde{a}_n$ מקיימת את הנדרש. ■

חלק II
שדות

תזכורת: **שדה** הוא חוג חילוק קומוטטיבי.

5 הרחבת שדות

הגדרה: יהיו K,F שדות. נאמר כי K הוא **הרחבה** של F ונסמן $F\leq K$, אם F הוא תת־שדה של K.

כלומר אם F סגור כקבוצה תחת החיבור והכפל המוגדרים ב-K, ומכיל את $0,1$ של K. במילים אחרות, F הוא שדה בעצמו המהווה גם תת־חוג של K.

טענה: כל הופכי של איבר ב-F הוא ההופכי שלו ב-K.

הוכחה: יהי $a\in F$ ונניח כי $b\in F$ הופכי שלו ב-F וכי $a^{-1}\in K$ הופכי שלו ב-K. מתקיים כי $ab=1$ ב-F, ומהיות 1 איבר גם של K נובע כי $ab=1$ גם ב-K, ומיחידות ההופכי ב-K נובע כי $b=a^{-1}$. ■

הגדרה: בהינתן $F\leq K$, לכל $a\in K$ נסמן ב-$F\left[a\right]$ את תת החוג של K הנוצר על־ידי a,F. אוסף זה הוא בדיוק $\{f\left(a\right)|f\in F\left[x\right]\}$.[28]

כמו־כן, לכל $a\in K$ נסמן ב-$F\left(a\right)$ את תת השדה של K הנוצר על־ידי a,F. אוסף זה הוא בדיוק $\left\{\frac{f(a)}{g(a)}|f,g\in F\left[x\right],\,g\left(a\right)\neq 0\right\}$.

הערה: יהי F שדה ויהי R חוג המרחיב את F, כלומר F הוא תת־חוג של R, אז בפרט R הוא מרחב וקטורי מעל F.[29]

הגדרה: יהי F שדה המהווה תת־חוג של R. אומרים כי R הוא **הרחבה סופית** של F, אם הממד שלו כמרחב וקטורי מעל F הוא סופי. בסימון מקובל $\dim_F R<\infty$.

הערה: אנו נשתמש במושג זה בעיקר בהרחבות שדות. במקרה כזה נסמן $[K:F]=:\dim_F K$. למשל $[\mathbb{C}:\mathbb{R}]=\dim_{\mathbb{R}}\mathbb{C}=2$.

משפט: יהיו $F\leq K,\ K\leq L$ הרחבות שדות ששתיהן סופיות, ונסמן $\begin{array}{c}[K:F]=n\\ [L:K]=m\end{array}$.

קל לראות שבמקרה זה מוגדרת הרחבת השדות $F\leq L$. אזי גם הרחבת שדות זו היא סופית, ומתקיים $[L:F]=n\cdot m$.

הוכחה: מהנתון $F\leq K$ נובע שקיימים $a_1,...,a_n$ בסיס של K מעל F.

מהנתון $K\leq L$ נובע שקיימים $b_1,...,b_m$ בסיס של L מעל K.

נוכיח שהקבוצה $\left\{a_i\cdot b_j|\ \begin{array}{c}i=1,...,n\\ j=1,...,m\end{array}\right\}$ היא בסיס של L מעל F, כלומר פורשת ובלתי־תלויה לינארית, ובזאת נסיים שכן קל לראות שגודלה $n\cdot m$.

---

[28] כאשר $F\left[x\right]$ הוא חוג הפולינומים במשתנה אחד.

[29] מוגדר חיבור ב-R וכן $0,1\in R$. גם הכפל בסקלר $F\times R\to R$ קיים מאליו, כי הוא מתקבל מפעולת הכפל ב-R כחוג $R\times R\to R$ מצומצמת ל-F.

• <u>פורשת</u>: יהי $c\in L$. נתון ש-L מרחיב את K ולכן קיימים $x_1,...,x_m\in K$ כך ש-$c=x_1b_1+...+x_mb_m$.

נתון ש-K מרחיב את F ולכן לכל x_j, $1\le j\le m$, קיימים $y_{j1},...,y_{jn}\in F$ כך ש-$x_j=y_{j1}a_1+...+y_{jn}a_n$.

כעת מהצבת כל המשוואות יחד נובע כי c מתקבל כצירוף לינארי של הקבוצה $\left\{a_i\cdot b_j \middle| \begin{array}{c} i=1,...,n \\ j=1,...,m\end{array}\right\}$, כנדרש.

• <u>בת"ל</u>: נניח שעבור $r_{11},r_{12},r_{21},...,r_{nm}\in F$ כלשהם $\sum_{\substack{i=1,...,n\\ j=1,...,m}} r_{ij}a_ib_j=0$. נתייחס לביטוי זה כצירוף של $b_1,...,b_m\in L$ מעל K, כלומר:

$$\sum_{\substack{i=1,...,n\\ j=1,...,m}} r_{ij}a_ib_j=\underbrace{\left(\sum_{i=1,...,n} r_{i1}a_i\right)}_{\in K}b_1+...+\underbrace{\left(\sum_{i=1,...,n} r_{im}a_i\right)}_{\in K}b_m=0$$

מהיות $b_1,...,b_m$ בסיס של L מעל K נוכל להסיק שלכל $1\le j\le m$ מתקיים $\sum_{i=1,...,n} r_{ij}a_i=0$.

וכעת מהיות $a_1,...,a_n$ בסיס של K מעל F נוכל להסיק שלכל $1\le j\le m$ מתקיים לכל $1\le i\le n$ כי $r_{ij}=0$. ■

משפט: יהיו $F\le K$ שדות, $a\in K$. אם $F[a]$ הוא תת־חוג ממימד סופי מעל F, אז $F[a]$ הוא שדה. כלומר $F[a]=F(a)$.

באופן כללי יותר: לכל תחום שלמות D ולכל שדה F כך ש-$F\subset D$ ומתקיים $\dim_F D<\infty$, אז D הוא שדה.

הוכחה: נסמן $\dim_F D=n<\infty$ ויהי $0\ne d\in D$, צריך למצוא לו הופכי ב-D.

נגדיר העתקה $L:D\to D$ על־ידי $L(x)=dx$. קל לוודא שזו העתקה לינארית. כמו כן $\ker(L)=\{0\}$ מהיות D תחום שלמות, לכן L חח"ע.

ממשפט הממדים נובע כי $D\cong {}^{D}/_{\ker(L)}\cong L(D)$, ולכן $\dim_F L(D)=n$. אבל $L(D)$ הוא תת־מרחב של D, ולכן משוויון הממדים והאיזומורפיזם נובע שוויון ממש, כלומר $L(D)=D$.

נשים לב כי $1\in D$ ולכן גם $1\in L(D)$. מכאן שקיים $x\in D$ כך ש-$L(x)=1$, כלומר $dx=1$, ולכן ל-d יש הופכי. ■

5.1 איברים אלגבריים

הגדרה: תהי $F\le K$ הרחבת שדות ויהי $a\in K$. נאמר כי a הוא **איבר אלגברי** מעל F אם קיים פולינום $0\ne f\in F[x]$ המקיים $f(a)=0$.

איבר שאינו אלגברי מכונה **טרנסצנדנטי**.

הערה: כל $a\in F$ הוא ודאי אלגברי, כי הוא מאפס את הפולינום $f(x)=x-a$.

$\sqrt{2}\in\mathbb{Q}$ הוא אלגברי מעל $\mathbb{Z}$, כי הוא מאפס את הפולינום x^2-2. קשה באופן כללי למצוא איברים טרנסצנדנטיים. למשל e ו-π הם כאלה, אולם את ההוכחה לא נביא כאן.

הגדרה: לכל איבר אלגברי $a\in K$ מעל F, נגדיר את **דרגת האלגבריות** שלו להיות הדרגה המינימלית של איזשהו פולינום שהוא מאפס.

טענה: תהי $F\leq K$ הרחבת שדות ויהי $\alpha\in K$ איבר אלגברי מדרגה d. יהי גם $f\in F\left[x\right]$ פולינום כלשהו מדרגה d המקיים $f\left(\alpha\right)=0$.

אזי לכל פולינום $0\neq g\in F\left[x\right]$ המקיים $g\left(\alpha\right)=0$, מתקיים כי $f|g$.

הוכחה: נגדיר $I=:\left\{h\in F\left[x\right]|h\left(\alpha\right)=0\right\}$. ניתן לוודא שזה אידאל ב-$F\left[x\right]$. אבל מההגדרה נובע כי f הוא בעל דרגה מזערית ב-I, ולכן $I=\left(f\right)$, כלומר f יוצר את האידאל. לכן לכל g המקיים $g\left(\alpha\right)=0$, כלומר $g\in I$, מתקיים כי $f|g$. ■

מסקנה: כל זוג פולינומים $0\neq f_1,f_2\in F\left[x\right]$ שהם מדרגה d ומתאפסים לאיזשהו $\alpha\in K$ אלגברי מעל F מדרגה d, הם חברים. וזאת כי $f_1|f_2$ וגם $f_2|f_1$.

מסקנה: לכל $\alpha\in K$ איבר אלגברי מדרגה d מעל F, קיים פולינום <u>מתוקן</u> יחיד $f\in F\left[x\right]$ מדרגה d, המקיים $f\left(\alpha\right)=0$.

הגדרה: תהי $F\leq K$ הרחבת שדות ויהי $\alpha\in K$ איבר אלגברי מדרגה d. לפולינום המתוקן היחיד $f\in F\left[x\right]$ מדרגה d המקיים $f\left(\alpha\right)=0$, נקרא **הפולינום המזערי** של α.

משפט: תהי $F\leq K$ הרחבת שדות ויהי $\alpha\in K$, אזי התנאים הבאים שקולים:

1. α אלגברי מעל F.
2. $F\left[\alpha\right]$ תת־חוג ממימד סופי מעל F.
3. $F\left(\alpha\right)$ תת־שדה ממימד סופי מעל F.

אם מתקיימים תנאים אלו אז גם $\left[F\left(\alpha\right):F\right]=\dim_F F\left(\alpha\right)=\dim_F F\left[\alpha\right]=d$.[30]

הוכחה: $(2\Longleftarrow3)$ נניח כי $\dim_F F\left[\alpha\right]=d<\infty$. ממשפט קודם נובע שמסופיות הממד זה שדה, כלומר $F\left[\alpha\right]=F\left(\alpha\right)$, ולכן גם $\left[F\left(\alpha\right):F\right]=d$.

$(3\Longleftarrow1)$ נניח כי $\dim_F F\left(\alpha\right)=d<\infty$. נתבונן באיברים $1,\alpha,\alpha^2,...,\alpha^d$. אלו $d+1$ איברים במרחב שממדו d, ולכן קיימים $a_0,...,a_d\in F$ לא כולם 0, כך שמתקיים $a_0+a_1\alpha+...+a_d\alpha^d=0$. מכאן נובע שהפולינום $0\neq f\left(x\right)=a_0+a_1x+...+a_dx^d\in F\left[x\right]$, שהוא ממעלה d, מתאפס על־ידי α ולכן α אלגברי. כמו־כן נובע כי דרגת האלגבריות שלו היא לכל היותר d.

$(1\Longleftarrow2)$ יהי $\alpha\in K$ אלגברי מדרגה d ויהי $f\in F\left[x\right]$ הפולינום המזערי שלו. צריך להראות כי $\dim_F F\left[\alpha\right]<\infty$.

יהי V תת המרחב הווקטורי מעל F שנפרש על־ידי $1,\alpha,...,\alpha^{d-1}$. מכאן שממדו הוא לכל היותר d. מצד אחד ברור כי $V\subset F\left[\alpha\right]$. נראה שמתקיימת גם ההכלה ההפוכה ולכן $V=F\left[\alpha\right]$ ובכך נסיים.

למה: $\alpha V\subset V$

[30] השוויון הראשון הוא סימון בלבד. את השוויון השני והשלישי נוכיח.

הוכחת הלמה: מספיק להראות זאת על איברי הבסיס הפורש, כלומר יש להראות כי $\alpha\cdot1,\alpha\cdot\alpha,...,\alpha\cdot\alpha^{d-1}\in V$. לכל $d-1$ האיברים הראשונים זה מתקיים מהגדרת V. נראה זאת ל-α^d.

מההנחה $f(\alpha)=0$ עבור f מהצורה $f(x)=x^d+b_{d-1}x^{d-1}+...+b_0$, נוכל להסיק כי $\alpha^d=-b_{d-1}\alpha^{d-1}-...-b_0$, כלומר $\alpha^d\in V$. ■

כעת נסיק שמתקיים $\alpha^2V=\alpha(\alpha V)\subset\alpha V\subset V$ ובאינדוקציה $\alpha^nV\subset V$ לכל n טבעי. לכן $\alpha^n\in V$ לכל n טבעי.

אבל נשים לב כי $F[\alpha]=\operatorname{span}\left\{1,\alpha,\alpha^2,...,\alpha^n,...\right\}$ (המונומים הם בסיס לכל חוג פולינומים במשתנה אחד), ולכן $F[\alpha]\subset V$.

מצאנו שהתנאים 1,2,3 שקולים. שוויון הממדים שמוזכר בסוף המשפט נובע גם הוא, בגלל הסנדביץ' $\dim_F F[\alpha]\le d\le[F(\alpha):F]=\dim_F F[\alpha]$.[31] ■

מסקנה יסודית: תהי $F\le K$ הרחבת שדות. נסמן ב-A את אוסף האיברים האלגבריים של K שהם מעל F. אזי A שדה המקיים $F\le A\le K$.

הוכחה: יהיו $\alpha,\beta\in A$ אלגבריים מדרגות m,n בהתאמה מעל F. מהמשפט האחרון נובע שבפרט $L_1=:F[\alpha]$ שדה סופי מממד m מעל F. כלומר מתקיים $F\le L_1\le K$.

נשים לב כי אם $\beta\in K$ אלגברי מעל F אז הוא גם אלגברי מעל L_1 כהרחבה של F, ולכן נפעיל שוב את המשפט האחרון ונסיק כי $L_2=:L_1[\beta]$ שדה סופי ממד לכל היותר n מעל L_1. כלומר מתקיים $F\le L_1\le L_2\le K$.

הראינו לעיל שמתקיים $[L_2:F]=[L_2:L_1]\cdot[L_1:F]$ ולכן נובע $[L_2:F]\le n\cdot m$. כלומר L_2 היא הרחבה סופית מעל F ולכן היא שדה. נשים לב כי $\alpha,\beta\in L_2$ ולכן מתקיים כי $\alpha+\beta,\alpha\cdot\beta,\frac{\alpha}{\beta},\alpha^{-1}\in L_2$. אבל מהיות L_2 הרחבה סופית מעל F נובע שכל ההרחבות שלהם סופיות מעל F.[32] לכן כל הנ"ל אלגבריים, כלומר כולם ב-A, ולכן A שדה מהצורה $F\le A\le K$. ■

5.1.1 המספרים האלגבריים

רקע: "המספרים האלגבריים" הם האיברים האלגבריים של הרחבת השדות $\mathbb{Q}\le\mathbb{C}$. כלומר כל ה-$z\in\mathbb{C}$ כך שיש פולינום ב-$\mathbb{Q}[x]$ שמתאפס על z.

מסמנים את שדה המספרים האלגבריים ב-$\overline{\mathbb{Q}}$. כלומר $\mathbb{Q}\le\overline{\mathbb{Q}}\le\mathbb{C}$. נראה ש-$\overline{\mathbb{Q}}$ שדה בן־מניה.

הגדרה: הראינו לעיל שלכל $\alpha\in\overline{\mathbb{Q}}$ קיים פולינום מזערי מוגדר היטב. לכן נגדיר העתקה מהצורה $\min p:\overline{\mathbb{Q}}\to\mathbb{Q}[x]$ על־ידי כך שכל מספר אלגברי α מועתק לפולינום המזערי שלו.

הגדרה: לכל d טבעי, נגדיר את $\overline{\mathbb{Q}}_d$ להיות אוסף המספרים האלגבריים מדרגה אלגברית d. נגדיר צמצום של $\min p$ לתחום זה, כלומר היא העתקה לתוך אוסף הפולינומים המתוקנים והאי־פריקים מדרגה d.

[31] האי־שוויון הראשון נובע מהחלק $1\Longleftarrow2$, האי־שוויון השני נובע מהחלק $3\Longleftarrow1$, והשוויון האחרון נובע מהחלק $2\Longleftarrow3$.

[32] נשים לב כי α שייך להרחבה סופית כלשהי של F אם ורק אם $F[\alpha]$ הרחבה סופית של F. כיוון אחד ברור. בכיוון השני, שהוא הרלוונטי לנושא שלנו, אם α שייך להרחבה סופית E כלשהי של F אז $F[\alpha]\le E$, ולכן גם ההרחבה $F\le F[\alpha]$ סופית.

טענה: התמונה של $\min p|_{\overline{\mathbb{Q}}_d}$ היא כל הפולינומים ב-$\mathbb{Q}[x]$ ממעלה d, שהם מתוקנים ואי־פריקים.

הוכחה: יהי $f \in \mathbb{Q}[x]$ פולינום מתוקן ואי־פריק. צריך להראות שקיים מספר אלגברי כך ש-f הפולינום המזערי שלו. אבל בפרט $f \in \mathbb{C}[x]$ ו-$\mathbb{C}$ סגור אלגברית, לכן קיים $\alpha \in \mathbb{C}$ המקיים $f(\alpha) = 0$. כמו כן f הפולינום המזערי של α, כי לו היה $g \in \mathbb{Q}[x]$ המקיים $\deg(g) < \deg(f)$ וגם $g(\alpha) = 0$, היינו מקבלים כי $g|f$ (כפי שהראינו לעיל), בסתירה לאי־פריקות f. ■

טענה: לכל פולינום $f \in \mathbb{Q}[x]$ ממעלה d כלשהי, יש לכל היותר d מקורות תחת $\min p|_{\overline{\mathbb{Q}}_d}$.

הוכחה: פולינום ממעלה d מתפרק ל-d גורמים לינאריים מעל $\mathbb{C}$. כל גורם כזה יכול לאפס את הפולינום אולם ייתכן שיש שורש מריבוי גדול מ-1,[33] לכן בכל מקרה אין יותר מ-d שורשים לפולינום. כלומר אין יותר מ-d מקורות תחת $\min p|_{\overline{\mathbb{Q}}_d}$. ■

מסקנה: השדה $\overline{\mathbb{Q}}$ הוא בן־מניה.

הוכחה: ידוע כי $\mathbb{Q}$ בן־מניה, ולכן לכל d טבעי גם $\mathbb{Q}^d$ הוא בן־מניה. נשים לב כי $\overline{\mathbb{Q}}_d \cong \mathbb{Q}^d$,[34] ולכן גם $\overline{\mathbb{Q}}_d$ בן־מניה. קל לראות כי $\overline{\mathbb{Q}} = \bigcup_{d\in\mathbb{N}} \overline{\mathbb{Q}}_d$, כלומר הוא איחוד בן־מניה של קבוצות בנות־מניה ולכן בעצמו בן־מניה.[35] ■

משפט: יהי F שדה ממציין 0,[36] ויהי $0 \neq f \in F[x]$ פולינום אי־פריק עם שורש α. אזי הריבוי של α ב-f הוא 1.

במילים אחרות: לכל פולינום אי־פריק ממעלה n מעל שדה ממציין 0, קיימים n שורשים שונים. ההוכחה מושארת כתרגיל מודרך.

6 הומומורפיזם של שדות

תזכורת: יהיו R, S חוגים. נאמר כי העתקה $f : R \to S$ היא **הומומורפיזם של חוגים**, אם היא משמרת חיבור וכפל בין החוגים, ומתקיים $f(1) = 1$, $f(0) = 0$. אם f גם חח"ע ועל, נקרא לה **איזומורפיזם של חוגים**.

טענה: אם K, L שדות ו-$f : K \to L$ הומומורפיזם של חוגים ביניהם, אז f חח"ע.

לכן לעתים נקרא להומומורפיזם של חוגים בין שדות **שיכון**.

הוכחה: מתקיים כי $f(1) = 1$ ולכן $f^{-1}(0) \neq K$. מצד שני ידוע כי $f^{-1}(0) \lhd K$. אבל K שדה ולכן הוא חוג פשוט ולכן בהכרח $f^{-1}(0) = \{0\}$, כלומר הגרעין טריוויאלי ומכאן החח"ע. ■

הגדרה: יהיו $F \leq K_1$, $F \leq K_2$ שתי הרחבות שדות. נאמר כי הומומורפיזם $\jmath : K_1 \to K_2$ הוא **שיכון של הרחבות**, אם הוא משמר את F. כלומר אם לכל $a \in F$ מתקיים $f(a) = a$.

---

[33] ריבוי של שורש α הוא חזקת הגורם $x - \alpha$ בפירוק. למשל בפולינום $(x-\alpha)^2(x-\beta)$, הריבוי של השורש α הוא 2 והריבוי של השורש β הוא 1.

[34] למשל על־ידי ההעתקה $(a_0, a_1, ..., a_{d-1}) \mapsto a_0 + a_1 x + ... + a_{d-1}x^{d-1} + x^d$.

[35] הנחנו את אקסיומת הבחירה בהוכחה זו.

[36] כלומר שלא קיים m טבעי שעבורו $\underbrace{1 + 1 + ... + 1}_{m \text{ times}} = 0$.

מכיוון ש-$\jmath$ חח"ע ממילא, אם הוא גם על נקרא לו **איזומורפיזם של הרחבות**. נסמן לעתים שיכון של הרחבות על־ידי $\jmath : K_1 \underset{F}{\to} K_2$.

משפט: יהי F שדה ויהיו הרחבות השדות $F \leq F(\alpha)$, $F \leq F(\alpha')$ ל-α, α' אלגבריים (כך שההרחבה סופית). נניח עוד של-α, α' אותו פולינום מזערי.

אזי קיים איזומורפיזם של הרחבות $\jmath : F(\alpha) \underset{F}{\to} F(\alpha')$, שגם מקיים $\jmath(\alpha) = \alpha'$.

הוכחה: נסמן $\min p(\alpha) = \min p(\alpha') =: f \in F[x]$, ונראה ששני השדות איזומורפיים כשדות ל-${}^{F[x]}/_{(f)}$. מהיות הפולינום המזערי f מינימלי נובע שהוא אי־פריק ולכן ראשוני, לכן האידאל (f) מירבי (נזכור כי $F[x]$ תחום ראשי) ולכן חוג המנה הנ"ל הוא שדה.

נגדיר העתקה $\pi_\alpha : F[x] \to F(\alpha)$ להיות הערכה ב-α. כלומר לכל $g \in F[x]$ מגדירים $\pi_\alpha(g) = g(\alpha)$. קל לוודא שזה הומומורפיזם ו-$\pi_\alpha(F[x]) = F(\alpha)$.

מתקיים כי $\pi_\alpha^{-1}(0) = (f)$, שכן $f(\alpha) = 0$ וכן לכל פולינום $h \in F[x]$ המקיים $h(\alpha) = 0$ מתקיים $f|h$, כלומר $h \in (f)$. לכן ממשפט האיזומורפיזם לחוגים נסיק כי ${}^{F[x]}/_{(f)} \cong F(\alpha)$. באופן דומה גם ${}^{F[x]}/_{(f)} \cong F(\alpha')$.

לכן קיימים איזומורפיזמים של חוגים $\jmath_2 : {}^{F[x]}/_{(f)} \to F(\alpha')$, $\jmath_1 : {}^{F[x]}/_{(f)} \to F(\alpha)$, ומכאן כי $\jmath = \jmath_2 \circ \jmath_1^{-1}$ איזומורפיזם של החוגים $F(\alpha), F(\alpha')$.

נראה כי $\jmath$ איזומורפיזם של הרחבות, כלומר שהוא משמר את F. במשפט האיזומורפיזם, $\jmath_1$ מוגדר להיות $\jmath_1(g + (f)) = \pi_\alpha(g)$. כמו־כן $\pi_\alpha(a) = a$ לכל סקלר $a \in F$ בתפקיד של פולינום קבוע, ולכן $\jmath_1(a + (f)) = \pi_\alpha(a) = a$ לכל $a \in F$. באופן דומה גם $\jmath_2(a) = a$ לכל $a \in F$, ולכן ההרכבה $\jmath$ משמרת את F.

נותר להראות $\jmath(\alpha) = \alpha'$. נשים לב כי $\pi_\alpha(x) = \alpha$ ולכן $\alpha \overset{\jmath_1^{-1}}{\mapsto} x + (f) \overset{\jmath_2}{\mapsto} \alpha'$. ■

משפט: (הכללה של המשפט הקודם) יהי $\jmath : F \to F'$ איזומורפיזם של שדות ויהיו שתי ההרחבות $F' \leq K'$, $F \leq K$. יהי $\alpha \in K \backslash F$ איבר אלגברי ויהי $f = \min p(\alpha)$ מעל F. יהי גם $\alpha' \in K'$ שורש של $\bar{\jmath}(f)$.[37]

אזי קיים איזומורפיזם של הרחבות $\hat{\jmath} : F(\alpha) \underset{F}{\to} F'(\alpha')$ המקיים $\hat{\jmath}(\alpha) = \alpha'$.

הוכחה: מקיום האיזומורפיזם $\jmath : F \to F'$ נובע שקיים איזומורפיזם $\bar{\jmath} : F[x] \underset{F}{\to} F'[x]$.[38]

נסמן $f =: \min p(\alpha)$ ונשים לב שמתקיים $\bar{\jmath}((f)) = (\bar{\jmath}(f))$. לכן נוכל להגדיר את האיזומורפיזם $\jmath^* : {}^{F[x]}/_{(f)} \to {}^{F'[x]}/_{\bar{\jmath}((f))}$ על־ידי $\jmath^*(h + (f)) = \bar{\jmath}(h) + (\bar{\jmath}(f))$.

כעת נסיק:

$$F(\alpha) \cong {}^{F[x]}/_{(f)} \cong {}^{F'[x]}/_{\jmath((f))} \cong F'(\alpha')$$

כאשר האיזומורפיזם האמצעי הוא $\jmath^*$ שבנינו, והאיזומורפיזמים משמאל ומימין נובעים מהמשפט הקודם. לכן ההרכבה המתאימה היא איזומורפיזם $\hat{\jmath} : F(\alpha) \to F'(\alpha')$.

---

[37] כלומר הפעלת האיזומורפיזם $\jmath$ על מקדמי הפולינום f.

[38] כלומר הפעלת האיזומורפיזם $\jmath$ על מקדמי הפולינום.

נראה כי $\hat{\jmath}$ משמר את $F \cong F'$: לכל $a \in F$ מתקיים:

$$a \mapsto a + (f) \mapsto \bar{\jmath}(a) + (\bar{\jmath}(f)) = \jmath(a) + (\bar{\jmath}(f)) \mapsto \jmath(a)$$

נראה כי $\hat{\jmath}(\alpha) = \alpha'$. כפי שהראינו במשפט הקודם מתקיים $\alpha \mapsto x + (f)$. כמו־כן מתקיים:

$$x + (f) \mapsto \bar{\jmath}(x) + (\bar{\jmath}(f)) = \jmath(1)(x) + (\bar{\jmath}(f)) = x + (\bar{\jmath}(f))$$

ולכן בסך הכל מתקיים $\alpha \mapsto x + (f) \mapsto x + (\bar{\jmath}(f)) \mapsto \alpha'$. ■

הגדרה: תהי $F \leq K$ הרחבת שדות ויהי $f \in F[x]$. נאמר כי K הוא **שדה פיצול** של f, אם f **מתפצל** מעליו; כלומר אם יש $c, a_1, ..., a_d \in K$, לא בהכרח כולם שונים, כך ש-$f = c(x - a_1) \cdot ... \cdot (x - a_d)$.

בתנאים אלה, נאמר כי K הוא **שדה פיצול מזערי** אם לא קיימת תת־הרחבה ממש שהיא שדה פיצול של f.

הערה: נשים לב ש-K הוא שדה פיצול מזערי של f אם ורק אם קיים ל-f הפיצול $f = c(x - a_1) \cdot ... \cdot (x - a_d)$ ל-$a_1, ..., a_d \in K$ וגם $K = F(a_1, ..., a_d)$.

משפט: תהי $F \leq K$ הרחבת שדות, ויהי $f \in F[x]$ פולינום שיש לו שורשים $\alpha_1, ..., \alpha_n \in K$ (לאו דווקא כל השורשים שלו). יהי $\jmath : F \to L$ שיכון של הרחבות, ונניח כי $\bar{\jmath}(f) \in L[x]$ מתפצל מעל L. אזי קיים שיכון של הרחבות $F(\alpha_1, ..., \alpha_n) \underset{F}{\to} L$.

הוכחה: נגדיר $F_0 = F$ ורקורסיבית $F_k = F(\alpha_1, ..., \alpha_k)$. קל לראות כי $F_k = F_{k-1}(\alpha_k)$.

נגדיר $\jmath_0 = \jmath$, ורקורסיבית נגדיר בהתאמה $\jmath_k : F_k \underset{F}{\to} L$ באופן הבא: נניח כי $\jmath_{k-1} : F_{k-1} \underset{F}{\to} L$ מוגדר, אז נתבונן ב-$\bar{f} =: \bar{\jmath}(f)$ ונגדיר $g =: \min p(\alpha_k)$ מעל F_{k-1}. מאחר ומתקיים $f(\alpha_k) = 0$ נובע כי $g|f$ מעל F_{k-1}, ולכן $\bar{g} =: \bar{\jmath}(g)\,|\bar{f}$ ב-L.

מכך ש-$\bar{f}$ מתפצל ב-L נובע שגם $\bar{g}$ מתפצל ב-L, ובפרט יש לו שורש שם. לכן נובע ממשפט קודם שעבור $F_k = F_{k-1}(\alpha_k)$ קיים שיכון של הרחבות $\jmath_k : F_k \underset{F}{\to} L$.

אם כך הגדרנו רקורסיבית את $\jmath_n : F_n \underset{F}{\to} L$ ו-$F_n = F(\alpha_1, ..., \alpha_n)$, והוא האיזומורפיזם המבוקש. ■

משפט: יהי F שדה ויהי $f \in F[x]$. נסמן $d = \deg(f)$. אזי:

1. קיים שדה פיצול מזערי ל-f מעל F. כמו־כן אם נסמן שדה זה ב-K, מתקיים $[K : F] \leq d!$.
2. שדה הפיצול המזערי K הוא יחיד עד־כדי איזומורפיזם של הרחבות של F.

תזכורת: במהלך ההוכחה נשתמש ב**משפט קרונקר**:

לכל $f \in F[x]$, $1 < \deg(f)$, קיים שדה פיצול שמכיל שורש של f.

הוכחה:

1. נוכיח באינדוקציה על d. במקרה $d=1$ אז f פולינום לינארי ולכן כל השורשים שלו ב-F. כלומר F עצמו הוא שדה הפיצול המזערי, ואכן $[F:F]=1$.

ל-$d>1$ כללי, נסמן ב-F' את ההרחבה שמכילה α שהוא שורש כלשהו של f (קיים ממשפט קרונקר). ב-$F'[x]$ מתקיים $f=(x-\alpha)g$ ל-$g\in F'[x]$ המקיים $\deg(g)=d-1$. לכן מהנחת האינדוקציה קיים שדה פיצול $F'\leq K$ שמעליו g מתפצל. אבל גם $\alpha\in F'\leq K$ ולכן K שדה שמעליו גם f מתפצל.

כעת נשים לב שמתקיים $F\leq F'\leq K$ ולכן מהנחת האינדוקציה ומזהות שהראינו לעיל נובע $[K:F]=[K:F']\cdot[F':F]\leq(d-1)!\cdot d=d!$.

נותר להראות את מזעריות K. מהנחת האינדוקציה F' שדה פיצול מזערי של g. אבל $g|f$ ולכן כל שדה פיצול של f חייב להכיל את K. כמו כן השורש היחיד שאינו של g ושחסר כדי לפצל את f הוא α, ואכן $\alpha\in K$ ולכן K הוא המזערי.

2. ממזעריות K כשדה פיצול נובע כי K נוצר מעל F על־ידי כל שורשי f. יהי K' שדה פיצול מזערי אחר של f. מהמשפט הקודם נובע שקיים $\jmath:K\underset{F}{\to}K'$ שהוא שיכון של שדות.

אבל K נוצר על־ידי שורשי f שסימנו $\alpha,\beta_1,...,\beta_{d-1}$, ולכן ב-$K'$ מתקיים כי $\jmath(\alpha),\jmath(\beta_1),...,\jmath(\beta_{d-1})$ הם שורשי f, ולכן הם יוצרים את K'. אם כך קיבלנו שמדובר בשיכון שהוא על K' ומכאן כי $K\cong K'$. ■

7 בנייה באמצעות סרגל ומחוגה

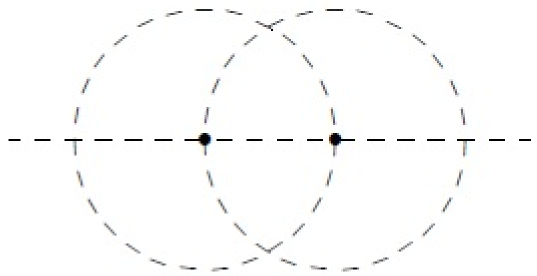
הגדרה: במישור $\mathbb{R}^2$, **סרגל** הוא הישר העובר דרך שתי נקודות כלשהן במישור, **ומחוגה** היא המעגל שמרכזו בנקודה כלשהי במישור ועובר דרך נקודה נוספת כלשהי במישור.

בהינתן קבוצה של נקודות במישור, **בנייה באמצעות סרגל ומחוגה** היא דרך לקבל מקבוצה זו נקודות נוספות במישור. בדרך זו מגדירים שלושה צעדים אפשריים לקבלת נקודה מתוך קבוצה נתונה:

- נקודת החיתוך של שני סרגלים של נקודות מהקבוצה
- נקודת החיתוך של סרגל ומעגל של נקודות מהקבוצה
- נקודת החיתוך של שני מעגלים של נקודות מהקבוצה

[39] אם נקודה מתקבלת לאחר ביצוע סדרה סופית כלשהי של צעדים כאלה, אומרים כי היא **ניתנת לבנייה באמצעות סרגל ומחוגה** מתוך קבוצת הנקודות הנתונה.

דוגמה: נסמן $\mathbb{R}^2 \supset \{(0,0),(0,1)\} =: P$. ל-$P$ יש ישר יחיד שעובר דרך שתי נקודותיה (ציר ה-x) ושני מעגלים שמרכזם הוא נקודה ב-P ועוברים דרך נקודה ב-P (זוג מעגלי יחידה סביב הנקודות הנ"ל). לפיכך קל לראות שבשלב הראשון ניתן על־ידי צעד אחד לבנות בסרגל ומחוגה עוד 4 נקודות, בנוסף על זוג הנקודות שב-P:



אם נמשיך את התהליך כל מספר סופי של צעדים, נקבל אינסוף נקודות נוספות.

את קבוצת כל הנקודות שניתן לבנות באמצעות סרגל ומחוגה מתוך P נסמן $E_{\mathbb{R}}$.

משפט: תהי $P = \{p_0, ..., p_m\} \subset \mathbb{R}^2$ קבוצה סופית. נסמן $p_i = (\alpha_i, \beta_i)$, $0 \leq i \leq m$, ונגדיר שדה הרחבה K להיות:

$$\mathbb{Q} \leq K =: \mathbb{Q}(\alpha_0, \beta_0, ..., \alpha_m, \beta_m) \leq \mathbb{R}$$

נגדיר את $\hat{P}$ להיות קבוצת נקודות סופית המתקבלת מנקודות P באמצעות בנייה בסרגל ומחוגה מספר סופי כלשהו של פעמים. נסמן $\hat{P} = \{p_0, ..., p_m, p_{m+1}, ..., p_n\}$,[40] ונגדיר בדומה שדה הרחבה $\hat{K}$ להיות:

$$\mathbb{Q} \leq \hat{K} = \mathbb{Q}(\alpha_0, \beta_0, ..., \alpha_m, \beta_m, \alpha_{m+1}, \beta_{m+1}, ..., \alpha_k, \beta_k) \leq \mathbb{R}$$

[39] נקודת השקה אינה מוגדרת נקודת חיתוך, אבל לא קשה להראות שבהינתן נקודה וישר, ניתן לקבל מהן את הנקודה על הישר שמשיקה למעגל ברדיוס המרחק בין הנקודה לישר.

[40] ברור כי $P \subset \hat{P}$

אזי מתקיים $\left[\hat{K}:K\right]=2^l$ ל-$0\le l$ כלשהו.

הוכחה: מספיק להראות שבכל תוספת של נקודה ממד ההרחבה הוא בהכרח 1 או 2, כלומר שמתקיים כי $[K_0(\alpha_{n+1},\beta_{n+1}):K_0]$ עבור $p_{n+1}=(\alpha_{n+1},\beta_{n+1})$. כי מכך נוכל להסיק איטרטיבית שלאחר מספר סופי של שלבים ממד ההרחבה יכול לגדול אך ורק בחזקות של 2.[41]

אם כך בהינתן נקודה חדשה $p_{n+1}=(x,y)$ שנבנתה באמצעות סרגל ומחוגה מתוך הקבוצה $\{p_0,...,p_n\}$, זה אומר שהיא חיתוך של שני ישרים, חיתוך של ישר ומעגל או של שני מעגלים. נראה שבכל אחד מהמקרים ממד ההרחבה של $K_0[x,y]$ מעל K_0 הוא בהכרח 1 או 2.

- נניח כי p_{n+1} נמצאת בחיתוך של שני ישרים, האחד עובר דרך נקודות שנסמן $(p,q),(r,s)$ והשני עובר דרך נקודות שנסמן $(z,w),(u,v)$.

  בשירטוט ניתן להיווכח שמהיות p_{n+1} בחיתוך שני הישרים מתקבלת מערכת המשוואות הלינארית $\begin{cases}\frac{x-p}{r-p}=\frac{y-q}{s-q}\\ \frac{x-z}{u-z}=\frac{y-w}{v-w}\end{cases}$. זו מערכת של שתי משוואות לינאריות בשני נעלמים, ולכן הפתרון שלה, $p_{n+1}=(x,y)$, נתון לפי נוסחת קרמר כמנת דטרמיננטות של מטריצות, כשרכיבי אותן מטריצות כולם לקוחים ממערכת המשוואות. דטרמיננטה היא כפל וחיבור של איברים בשדה ולכן הפתרון שייך לשדה K_0, מכאן שממד ההרחבה יהיה 1.

- נניח כי p_{n+1} נמצאת בחיתוך של ישר ומעגל, כאשר הישר עובר דרך נקודות שנסמן $(p,q),(r,s)$, ומרכז המעגל היא הנקודה שנסמן (u,v). נסמן את רדיוס המעגל ב-w.

  בשירטוט ניתן להיווכח שמהיות p_{n+1} על הישר מתקבלת המשוואה $\frac{x-p}{r-p}=\frac{y-q}{s-q}$ (כמו במקרה הקודם), וכן מהיות p_{n+1} על המעגל מתקבלת המשוואה $w^2=(x-u)^2+(y-v)^2$. מהמשוואה האחרונה נובע כי $w^2\in K_0$.

  מהמשוואה הראשונה נובע כי $y=\frac{s-q}{r-p}(x-p)+q$, ואם נציב שוויון זה במשוואה השנייה נקבל פולינום ריבועי ב-x:

$$K_0\ni w^2=(x-u)^2+\left(\frac{s-q}{r-p}(x-p)+q-v\right)^2$$

  אם לפולינום זה קיים שורש ב-K_0 אז ממד ההרחבה הוא 1. אם לפולינום זה לא קיים שורש ב-K_0 אז הוא אי־פריק, ולכן דרגת ההרחבה היא 2.

- המקרה בו p_{n+1} נמצאת בחיתוך של שני מעגלים ניתן להוכחה באופן דומה. ■

מסקנה 1: נניח כי שדה הקואורדינטות המתאים לקבוצה $P\subset\mathbb{R}$ הוא $\mathbb{Q}$ (כלומר $K=\mathbb{Q}$ בסימוני המשפט האחרון), ויהי $\alpha\in\mathbb{R}$ איבר אלגברי שמאפס פולינום אי־פריק $p(x)\in\mathbb{Q}[x]$.

אם הדרגה של $p(x)$ איננה חזקת 2, אז α איננו קואורדינטה של נקודה $\hat{p}$ המתקבלת מנקודות P באמצעות בנייה בסרגל ומחוגה.

[41] נזכור משפט שראינו: אם נתונה הרחבת שדות סופית $F_1\le F_2\le F_3$, אז $[F_3:F_1]=[F_3:F_2]\cdot[F_2:F_1]$.

הוכחה: נניח בשלילה שהנקודה $\hat{p}=(\alpha,\beta)$ ל-$\beta\in\mathbb{R}$ כלשהי מתקבלת בבנייה באמצעות סרגל ומחוגה מנקודות P. מהמשפט נובע שהשדה $\hat{K}=\mathbb{Q}(\hat{p})$ מקיים $\left[\hat{K}:\mathbb{Q}\right]=2^{l}$ ל-$0\leq l$. מתקיים $\hat{p}\in\hat{P}$ ולכן בפרט נובע $\alpha\in\hat{K}$. ברור שמתקיים $\mathbb{Q}\leq\mathbb{Q}(\alpha)\leq\hat{K}$ ולכן ממשפט שהראינו לעיל נובע:

$$2^{l}=\left[\hat{K}:\mathbb{Q}\right]=\left[\hat{K}:\mathbb{Q}(\alpha)\right]\cdot\left[\mathbb{Q}(\alpha):\mathbb{Q}\right]$$

מההנחה נובע $\deg(p(x))\neq 2^{l}$ ולכן $[\mathbb{Q}(\alpha):\mathbb{Q}]$ איננו חזקת 2. קיבלנו סתירה, כי כל גורמי חזקת 2 הם חזקת 2. ■

מסקנה 2: לא ניתן ליצור מקוביית היחידה קובייה שנפחה כפול, באמצעות סרגל ומחוגה. כלומר מנקודות $E_{\mathbb{R}}$ לא ניתן לקבל את הנקודה $\sqrt[3]{2}$ באמצעות סרגל ומחוגה.

הוכחה: אם בשלילה ניתן היה לעשות זאת אז היה $\sqrt[3]{2}\in\hat{K}$, עבור $\hat{K}$ השדה הסופי הנוצר על־ידי אוסף הנקודות שבנינו כדי לקבל את הקובייה בעלת הנפח הכפול.

נשים לב כי $\sqrt[3]{2}$ הוא שורש של הפולינום $p(t)=t^{3}-2$, שמקריטריון אייזנשטיין נובע כי הוא אי־פריק מעל $\mathbb{Q}$, ופולינום זה הוא ממעלה 3 שכמובן אינה חזקת 2. לכן לפי מסקנה 1 נקבל סתירה. ■

מסקנה 3: לא ניתן לחלק את הזווית $\frac{\pi}{3}$ (60°) ל-3 זוויות שוות, באמצעות סרגל ומחוגה.

הוכחה: נניח בשלילה שניתן לבנות את הזווית $\frac{\pi}{9}$. כלומר שניתן לקבל בבנייה באמצעות סרגל ומחוגה את הנקודה $\left(\cos\frac{\pi}{9},\sin\frac{\pi}{9}\right)$ מנקודות $E_{\mathbb{R}}$.

מתקיימת הזהות $\cos(3\theta)=4\cos^{3}\theta-3\cos\theta$ לכל θ.[42] לכן עבור $\theta=\frac{\pi}{9}$ נקבל:

$$\tfrac{1}{2}=\cos\left(\tfrac{\pi}{3}\right)=\cos\left(3\cdot\tfrac{\pi}{9}\right)=4\cos^{3}\left(\tfrac{\pi}{9}\right)-3\cos\left(\tfrac{\pi}{9}\right)$$

$$\Downarrow$$

$$2^{3}\cos^{3}\left(\tfrac{\pi}{9}\right)-3\cdot 2\cos\left(\tfrac{\pi}{9}\right)-1=0$$

נסמן $\alpha=2\cos\left(\frac{\pi}{9}\right)$, ונקבל כי α הוא שורש של הפולינום $p(t)=t^{3}-3t-1$. נראה כי $p(t)$ הפולינום המינימלי של α מעל $\mathbb{Q}$.

נציב $t=u+1$ ונקבל:

$$p(u+1)=(u+1)^{3}-3(u+1)-1=u^{3}+3u^{2}+3u+1-3u-3-1=u^{3}+3u^{2}-3$$

ומקריטריון אייזנשטיין ניתן להסיק כי הוא אי־פריק,[43] ופולינום זה הוא ממעלה 3 שכמובן אינה חזקת 2. לכן לפי מסקנה 1 נקבל סתירה. ■

מסקנה 4: לא ניתן לרבע את המעגל. כלומר מנקודות $E_{\mathbb{R}}$ לא ניתן לקבל את הנקודה $\sqrt{\pi}$ באמצעות סרגל ומחוגה.

---

[42] זה נובע מהזהות $\cos(\alpha+\beta)=\cos\alpha\cos\beta-\sin\alpha\sin\beta$, ע"י הצבת $\alpha=2\theta$, $\beta=\theta$.

[43] קל לראות שהצבה מסוג זה אינה משנה לאי־פריקות של פולינום.

הוכחה: לצורך הוכחת הטענה נשתמש במשפט שלא הוכחנו, לפיו π הוא מספר טרנסצנדנטי. כלומר אינו שורש של אף פולינום במקדמים רציונליים.

ממשפט זה נובע גם כי $\sqrt{\pi}$ טרנסצנדנטי. כי לו $\sqrt{\pi}$ היה שורש של פולינום במקדמים רציונליים, מכך שמתקיים $\mathbb{Q} \leq \mathbb{Q}(\pi) \leq \mathbb{Q}(\sqrt{\pi})$ ניתן היה להסיק:

$$\left[\mathbb{Q}\left(\sqrt{\pi}\right) : \mathbb{Q}(\pi)\right] \cdot \left[\mathbb{Q}(\pi) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{\pi}\right) : \mathbb{Q}\right] < \infty$$

אבל π טרנסצנדנטי ולכן $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$, ולכן זה לא ייתכן.

מהיות $\sqrt{\pi}$ טרנסצנדנטי, נובע בפרט שהוא גם אינו שורש של אף פולינום מדרגה שהיא חזקת 2. כלומר הוא אינו באף הרחבת שדות מדרגה שהיא חזקת 2. לכן מהמשפט שהראינו נובע שלא ייתכן שהוא ניתן לבנייה באמצעות סרגל ומחוגה. ■

8 נגזרת פורמלית

הגדרה: יהי F שדה כלשהו ויהי $f \in F[x]$ מהצורה $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$. נגדיר את **הנגזרת** שלו $f' \in F[x]$ להיות:

$$f'(x) = na_n x^{n-1} + (n-1)\, a_{n-1} x^{n-2} + ... + a_1$$

הערה:

- אם $charF = 0$ אז $f' = 0 \iff f = a_0$.
- אם $charF = p > 0$ התכונה הקודמת לא נכונה,[44] אולם $f(x) = g(x^p) \iff f' = 0$ ל-$g \in F_p[x]$. כלומר $f' = 0$ אם ורק אם כל החזקות המופיעות ב-f הן כפולות p.

תכונות בסיסיות: לכל $f, g \in F[x]$ מתקיים:

1. $(f+g)' = f' + g'$
2. $(cf') = cf'$ לכל $c \in F$
3. $(fg)' = f'g + fg'$

(ההוכחה מושארת כתרגיל)

טענה: לפולינומים $f, f' \in F[x]$ קיים גורם משותף לא טריוויאלי (כלומר לא קבוע) אם ורק אם ל-f קיים שורש מריבוי גדול מ-1.

הוכחה: (כיוון ראשון) נניח של-f קיים שורש α_0 מריבוי גדול מ-1. אזי ניתן להציג $f(x) = (x-\alpha_0)^2 (x-\alpha_1) ... (x-\alpha_{n-1})$ מעל שדה הפיצול. מהתכונה השלישית של נגזרת קל לראות ש-$x - \alpha_0$ הוא גם גורם של f', ועל־כן קיים ל-f, f' שורש משותף בשדה הפיצול. נראה שבאופן כללי קיום גורם משותף בשדה הפיצול גורר קיום גורם משותף בשדה המקורי.

---

[44] למשל ל-$f(x) = x^p \in F_p[x]$ מתקיים $f' = 0$.

אם ל-f, f' אין גורמים משותפים ב-F, כלומר הם זרים ומתקיים $\gcd(f, f') = 1$, אז מהלמה של בזו נובע שקיימים פולינומים $a(x), b(x)$ המקיימים $a(x) f(x) + b(x) f'(x) = 1$. המשמעות של שוויון זה מעל שדה הפיצול היא ש-f, f' זרים גם בשדה הפיצול, כלומר שאין להם גורם משותף בשדה הפיצול.

(כיוון שני) נניח של-f אין שורש מריבוי גדול מ-1. אזי ניתן להציג $f(x) = (x - \alpha_0)(x - \alpha_1) \ldots (x - \alpha_n)$ מעל שדה הפיצול, כאשר $\alpha_i \neq \alpha_j$ לכל $i \neq j$. מהתכונה השלישית של נגזרת נסיק כי הנגזרת של f היא מהצורה:

$$f'(x) = \sum_{i=1}^{n} (x - \alpha_0) \ldots \widehat{(x - \alpha_i)} \ldots (x - \alpha_n)$$

כאשר הסימון $\widehat{(x - \alpha_i)}$ מבטא את זה שגורם זה <u>אינו</u> במכפלה.

מכאן שלכל α_k שהוא שורש של f קיים האיבר $(\alpha_k - \alpha_0) \ldots \widehat{(\alpha_k - \alpha_k)} \ldots (\alpha_k - \alpha_n)$ בסכום שמגדיר את f' שלא מתאפס, ולכן כל שורש של f בהכרח אינו שורש של f'.

לו היה ל-f, f' גורם משותף לא טריוויאלי היה להם גם שורש משותף מעל שדה הפיצול, בסתירה לטיעון שהראינו, ולכן אין להם גורם משותף לא טריוויאלי. ■

מסקנה: אם $f \in F[x]$ פולינום אי־פריק ממעלה גדולה מ-0, אזי:

1. אם $charF = 0$ אזי כל שורשי f הם מריבוי 1.
2. אם $charF = p > 0$ אזי ל-f קיים שורש מריבוי גדול מ-1 אם ורק אם $f(x) = g(x^p)$. כלומר אם ורק אם כל החזקות המופיעות ב-f הן כפולות p.

הוכחה: נסמן $\deg f = n > 0$ כך ש-$\deg f' = n - 1$.

1. אם בשלילה היה ל-f שורש מריבוי גדול מ-1 אז מטענה קודמת היה ל-f, f' גורם משותף, כלומר קיים $g \in F[x]$, $0 < \deg g < n$, המקיים $g|f$, בסתירה לאי־פריקות f.
2. (בכיוון ראשון) אם $f' \neq 0$ (כלומר לא קיים g כנ"ל) אז ל-f, f' אין גורם משותף (אחרת f היה פריק) ולכן לא קיים ל-f שורש מריבוי גדול מ-1.
(בכיוון שני) אם $f' = 0$ (כלומר קיים g כנ"ל) אז $\gcd(f, f') = \gcd(f, 0) = f$ ולכן יש ל-f, f' גורם משותף. מהטענה נובע כי קיים ל-f שורש מריבוי גדול מ-1. ■

דוגמה: ניקח את השדה $\mathbb{F}_2$ המקיים $char\mathbb{F}_2 = 2$. נתבונן בשדה הפונקציות הרציונליות מעליו:

$$\mathbb{F}_2(x) =: \left\{ \frac{f(x)}{g(x)} | f, g \in \mathbb{F}_2[x], \ \forall_x \, g(x) \neq 0 \right\}$$

נגדיר $h \in \mathbb{F}_2(x)[u]$ על־ידי $h(u) = u^2 - x$. זהו פולינום ריבועי ולכן כדי להראות שהוא אי־פריק די להראות שאין לו שורש.

אם ל-h היה שורש כלשהו $\frac{f(x)}{g(x)} \in \mathbb{F}_2(x)$ אז היה מתקיים $\left(\frac{f(x)}{g(x)}\right)^2 - x = 0$ ולכן $f^2(x) = x g^2(x)$. אבל זה לא ייתכן כי כל המעלות מימין הן אי־זוגיות וכל המעלות משמאל זוגיות.

חלק III

תורת גלואה

9 הרחבות נורמליות

הגדרה: שדה F נקרא **מושלם**, באחד משני המקרים הבאים: $charF=0$, או $charF=p$ ל-p ראשוני וגם ההעתקה $F\to F$ מהצורה $a\mapsto a^p$ היא העתקה על.

הגדרה: יהי F שדה מושלם. הרחבת שדות סופית $F\leq K$ נקראת **הרחבה נורמלית**, אם כל פולינום אי־פריק $f\in F[x]$ שיש לו שורש כלשהו ב-K, מתפצל מעל K.

הערה: כשנכתוב "שדה הפיצול" של פולינום נתכוון לשדה המזערי בו הפולינום מתפצל.

טענה: הרחבה סופית $F\leq K$ ל-F מושלם היא הרחבה נורמלית, אם ורק אם לכל $\alpha\in K$ הפולינום המינימלי שלו מתפצל מעל K.

הוכחה: הכיוון הראשון מתקבל כמקרה פרטי. בכיוון השני, בהינתן $g\in F[x]$ פולינום אי־פריק כלשהו בעל שורש $\alpha\in K$, מאי הפריקות שלו נובע כי g (מתוקן) הוא הפולינום המינימלי של α. ■

דוגמאות:

1. F הוא הרחבה נורמלית מעל עצמו. וזאת כי אם $f\in F[x]$ אי־פריק וגם $a\in F$ שורש של f, בהכרח $f(x)=x-a$, כלומר הוא מתפצל.
2. הרחבת שדה על־ידי הסגור האלגברי שלו, אם היא סופית אז היא הרחבה נורמלית, מהגדרת הסגור האלגברי.
3. כל הרחבה ממימד 2 היא נורמלית:
   נניח כי $F\leq K$ הרחבה ממימד 2 וכן $charF\neq 2$. כלומר לכל $\alpha\in K\backslash F$ מתקיים $K=F(\alpha)$. כל α כזה הוא שורש של פולינום ריבועי x^2+bx+c ולכן הוא מהצורה $\alpha_{1,2}=\frac{-b\pm\sqrt{b^2-4a}}{2}$ (כאן משתמשים בהנחה $charF\neq 2$). מכאן נקבל את שני השורשים של הפולינום הריבועי, ולכן הוא מתפצל לגמרי ב-K.
4. הרחבה ממימד 3 אינה בהכרח נורמלית:
   ניקח למשל את ההרחבה $\mathbb{Q}\leq\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$ המתקבלת מהפולינום x^3-2 (אי־פריק לפי קריטריון אייזנשטיין), כאשר $\alpha_{1,2,3}=\sqrt[3]{2}$. נסמן את α_1 כשורש הממשי (היחיד).
   מתקיים $\mathbb{Q}(\alpha_1)\subsetneqq\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$, כי שדה הפיצול כולל גם מספרים מרוכבים. לכן x^3-2 לא מתפצל מעל $\mathbb{Q}(\alpha_1)$ למרות ש-α_1 שורש שלו.

תזכורת:

- בהינתן חוג R, מגדירים את $End(R)$ כאוסף ההומומורפיזמים $R\to R$, המכונים **אנדומורפיזמים**. אוסף זה מהווה חבורה ביחס לפעולת ההרכבה.
  תת החבורה $Aut(R)\leq End(R)$ היא אוסף ההומומורפיזמים החח"ע $R\to R$, המכונים **אוטומורפיזמים**.

- **אוטומורפיזם של הרחבת שדות** $F \leq K$ הוא אוטומורפיזם $\sigma : K \to K$ שקבוע על F. כלומר $\sigma(a) = a$ לכל $a \in F$.

  אוסף האוטומורפיזמים הללו מסומן ב-$Aut\left({}^{K}/_{F}\right)$, וגם הוא תת־חבורה.

  הערה: בשדות אין הבדל בין אנדומורפיזם לאוטומורפיזם, כי כל הומומורפיזם של שדות הוא חח"ע.

משפט: תהי $F \leq K$ הרחבת שדות סופית, אזי התנאים הבאים שקולים:

1. K שדה הפיצול (כלומר מזערי) של פולינום כלשהו $g \in F[x]$.
2. לכל הרחבה $K \leq L$ (סופית או לא) ולכל אוטומורפיזם של הרחבת שדות $\sigma \in Aut\left({}^{L}/_{F}\right)$ מתקיים $\sigma(K) \subset K$.

   הערה: בתנאים אלה $\sigma(K) = K \iff \sigma(K) \subset K$.
   כי אם $\sigma(K) \subset K$ לכל אוטומורפיזם, אז בפרט גם לאוטומורפיזם σ^{-1} (קיים מחח"ע σ) מתקיים $\sigma^{-1}(K) \subset K$, ולכן גם $K \subset \sigma(K)$ ומכאן השוויון.
3. ההרחבה $F \leq K$ היא נורמלית.

לצורך ההוכחה נוכיח טענת עזר כללית:

למה: לכל הרחבה סופית $F \leq K$ קיימת הרחבה סופית $K \leq L$, כך ש-L היא שדה הפיצול של פולינום כלשהו $h \in F[x]$.

הוכחה: מהיות ההרחבה סופית נובע כי K נוצר מעל F על־ידי מספר סופי של איברים. נסמן $K = F(a_1, ..., a_n)$ ל-$a_i \in K \backslash F$.

אלו איברים אלגבריים, ולכן לכל a_i קיים פולינום מינימלי $f_i \in F[x]$ המקיים $f_i(a_i) = 0$. נגדיר $h = f_1 \cdot ... \cdot f_n \in F[x]$.

יהי L שדה הפיצול של h מעל K. נרצה להראות שהוא גם שדה הפיצול של h מעל F.

יהי L' שדה ביניים $L' \leq L$ המכיל את F ואת כל שורשי h. נראה כי $L' = L$ ובזאת נסיים.

אבל $a_i \in L'$ ולכן $K = F(a_1, ..., a_n) \subset L'$, ומהמינימליות נובע $L' = L$. ■

הוכחה: $(1 \Longleftarrow 2)$

נסמן את הפיצול מעל K על־ידי $g(x) = (x - \alpha_1) ... (x - \alpha_n)$ ל-$\alpha_i \in K$ (נניח ללא הגבלת הכלליות כי g מתוקן). ממזעריות K נובע כי $K = F(\alpha_1, ..., \alpha_n)$.

תהי $K \leq L$ הרחבה ויהי $\sigma \in Aut\left({}^{L}/_{F}\right)$. נשים לב שלכל α_i גם $\sigma(\alpha_i)$ שורש של g, וזאת כי אם נסמן $g = x^n + b_{n-1}x^{n-1} + ... + b_0$ ל-$b_i \in F$, אז $\sigma(b_i) = b_i$.

מכאן כי אם $g(\alpha_i) = 0$ אז מהיות σ הומומורפיזם נובע:

$$0 = \sigma(0) = \sigma(g(\alpha_i)) = \sigma(\alpha_i^n) + \sigma\left(b_{n-1}\alpha_i^{n-1}\right) + ... + \sigma(b_0) =$$

$$= \sigma(\alpha_i)^n + b_{n-1}\sigma(\alpha_i)^{n-1} + ... + b_0$$

מכאן נובע שלכל $1 \leq i \leq n$ קיים $1 \leq j \leq n$ כך ש-$\sigma(\alpha_i) = \alpha_j$.

לכן $K=F\left(\alpha_1,...,\alpha_n\right)=F\left(\sigma\left(\alpha_1\right),...,\sigma\left(\alpha_n\right)\right)$, ומכך ש-$\sigma$ הומומורפיזם נסיק:

$$\sigma\left(K\right)=\sigma\left(F\left(\alpha_1,...,\alpha_n\right)\right)\subset F\left(\sigma\left(\alpha_1\right),...,\sigma\left(\alpha_n\right)\right)=K$$

($2\Longrightarrow 3$)

נוכיח מתוך 2 את התנאי השקול להרחבה נורמלית שהזכרנו לעיל: תהי $F\leq K$ הרחבת שדות סופית ויהי $a\in K$ עם הפולינום המינימלי שלו $f=:\min p\left(a\right)\in F\left[x\right]$. צריך להראות ש-$f$ מתפצל ב-K.

נבחר הרחבה $K\leq L'$ סופית כלשהי שהיא מספיק גדולה כך שמעליה f מתפצל. מלמה שהראינו לעיל נובע שקיימת הרחבה $K\leq L'\leq L$ כך ש-L היא שדה הפיצול של $h\in F\left[x\right]$ כלשהו.

אם כך קיבלנו הרחבה $K\leq L$ שהיא שדה הפיצול של $h\in F\left[x\right]$ כלשהו וגם שמעליה f מתפצל.

נראה מיד שלכל a' שורש אחר של f, קיים $\sigma\in Aut\left({}^{L}/_{F}\right)$ המקיים $\sigma\left(a'\right)=a\in K$. זה יסיים את ההוכחה, כי מההנחה $\sigma\left(K\right)=K$ נובע כי גם $a'\in K$, כלומר כל שורשי f ב-K, כנדרש.

למה: יהיו $F\leq K\leq L$ הרחבות סופיות, יהי $f\in F\left[x\right]$ שמתפצל ב-L ונניח עוד כי L הוא שדה הפיצול של $h\in F\left[x\right]$ כלשהו מעל F. אזי לכל שורשים $\alpha,\beta\in L$ של f, קיים אוטומורפיזם $\sigma\in Aut\left({}^{L}/_{F}\right)$ המעתיק $\alpha\mapsto\beta$.

הוכחת הלמה: הראינו באופן כללי שבהינתן פולינום אי־פריק $f\in F\left[x\right]$ וזוג שורשים שלו α,β בשדה הרחבה כלשהו, קיים איזומורפיזם $\jmath:F\left(\alpha\right)\to F\left(\beta\right)$ המקיים $\alpha\mapsto\beta$.

מהיות L שדה הפיצול של h כלשהו מעל F, נובע כי L שדה הפיצול של h גם מעל שדות הביניים $F\left(\alpha\right),F\left(\beta\right)$. ממשפט שהוכחנו לעיל קיים אוטומורפיזם של הרחבות $J:L\to L$ שמרחיב את $\jmath$ ולכן מעתיק $\alpha\mapsto\beta$, וזה האוטומורפיזם המבוקש. ■

($3\Longrightarrow 1$)

תהי $F\leq K$ הרחבה סופית נורמלית, לכן ניתן לסמן $K=F\left(a_1,...,a_n\right)$. לכל a_i קיים פולינום מינימלי $f_i\left(a_i\right)=0$, ומנורמליות ההרחבה $F\leq K$ נובע שכל f_i מתפצל מעל K.

נגדיר $f=f_1\cdot...\cdot f_n\in F\left[x\right]$. מכך שכל f_i מתפצל מעל K נובע כי f מתפצל מעל K. המזעריות נובעת מכך ששורשי f כוללים את כל $a_1,...,a_n$, ולכן כל שדה פיצול של f חייב להכיל את K. ■

10 התאמת גלואה

הגדרות:

- יהי F שדה מושלם ותהי $F \leq L$ הרחבה סופית ונורמלית. הרחבה כזאת נקראת **הרחבת גלואה**.
- **חבורת גלואה** של הרחבת גלואה כנ"ל, היא הקבוצה $Aut\left(L/F\right)$ עם פעולת ההרכבה.
  - בפרק הקרוב נראה כי ההתאמה הטבעית $K \mapsto Aut\left(L/K\right)$ בין אוסף שדות הביניים של ההרחבה $F \leq L$ לבין אוסף תתי החבורות של $Aut\left(L/F\right)$, המכונה **התאמת גלואה**, היא חח"ע ועל.

משפט (חלק א' של התאמת גלואה): תהי $F \leq L$ הרחבת גלואה ויהי K שדה ביניים.

נגדיר $H = Aut\left(L/K\right)$ ונגדיר עוד $K' = fix\left(H\right) =: \{a \in L | \forall_{\sigma \in H}\, \sigma\left(a\right) = a\}$.

אזי מתקיים $K = K'$.

מסקנה: ההתאמה בין שדות הביניים לתתי החבורות $K \mapsto Aut\left(L/K\right)$, היא חח"ע.

כי אם K_1, K_2 שדות ביניים המועתקים לאותה תת־חבורה $H \leq Aut\left(L/F\right)$, ניתן להפעיל את ההעתקה ההפוכה fix ולקבל כי $K_1 = K_2$.

הוכחה: נראה כי $K = K'$ על־ידי הכלה הדדית.

$K \subset K'$: יהי $a \in K$. מההגדרה $H = Aut\left(L/K\right)$ נובע $a \in fix\left(H\right) = K'$.

$K' \subset K$: נראה שאם $a \notin K$ אז $a \notin K'$.

המשמעות של $a \notin K'$ היא שקיים אוטומורפיזם $\sigma \in H$ כך ש-$\sigma\left(a\right) \neq a$.

נסמן את הפולינום המינימלי של a ב-$K\left[x\right]$ $f =: \min p\left(a\right) \in K\left[x\right]$.

אם $f\left(x\right) = x - a$ אז $a \in K$ וזו סתירה, לכן נניח $\deg\left(f\right) > 1$.

מכך שההרחבה $F \leq L$ נורמלית נובע שכל שורשי f מצויים ב-L.

יהי $a' \in L$ שורש נוסף של f ($\deg\left(f\right) > 1$) השונה מ-a.

f אי־פריק, ולכן כפי שהוכחנו לעיל קיים $\sigma \in Aut\left(L/K\right)$ המקיים $\sigma\left(a\right) = a'$, כלומר $\sigma\left(a\right) \neq a$, כנדרש. ■

טענה: חבורת גלואה של הרחבת גלואה, היא סופית.

מסקנה: להרחבה סופית של שדה מושלם, לאו דווקא נורמלית, יש מספר סופי של שדות ביניים.

הוכחת המסקנה: תהי $F \leq M$ הרחבה כנ"ל. הראינו לעיל שתמיד קיימת הרחבה סופית $M \leq L$ כך ש-L שדה הפיצול של פולינום $h \in F\left[x\right]$ כלשהו. לכן מהאיפיון הראשון לנורמליות נובע כי $F \leq L$ הרחבה נורמלית.

הראינו שקיימת העתקה חח"ע משדות ביניים $F \leq L$ לתתי החבורות של חבורת גלואה $Aut\left(L/F\right)$. לכן להרחבה $F \leq L$ יש מספר סופי של שדות ביניים, ומכאן ברור שגם להרחבה $F \leq M\left(\leq L\right)$ יש מספר סופי של שדות ביניים. ■

הוכחה: תהי $F \leq L$ הרחבת גלואה. נסמן $L = F(a_1, ..., a_n)$, $a_i \in L$.

לכל a_i קיים הפולינום המינימלי המתאים $f_i \in F[x]$. נגדיר $f = f_1 \cdot ... \cdot f_n$, ונקבל שכל a_i הוא שורש של f.

ל-f אולי קיימים שורשים נוספים ב-L, אז נגדיר את S להיות קבוצת כל השורשים של f ב-L. מתקיים כי $S \subset L$ תת־קבוצה סופית.

באופן כללי שורשי פולינום נשמרים תחת הומומורפיזם,[45] ולכן לכל $\sigma \in Aut(L/F)$ מתקיים $\sigma(S) = S$.

נגדיר העתקה $Aut(L/F) \to Sym(S)$ על־ידי $\sigma \mapsto \sigma|_S$. נשים לב שהתחום והטווח של העתקה זו הן חבורות, וכן היא הומומורפיזם של חבורות.[46]

מספיק להראות שהומומורפיזם זה חח"ע, ומכאן נסיק $|Aut(L/F)| \leq |Sym(S)| = |S|!$, כלומר חבורת גלואה סופית.[47]

למה: להעתקה $Aut(L/F) \to Sym(S)$ המוגדרת על־ידי $\sigma \mapsto \sigma|_S$ יש גרעין טריוויאלי, ולכן היא חח"ע.

הוכחת הלמה: יהי $\sigma \in Aut(L/F)$ בגרעין של ההעתקה הנ"ל. מההגדרה של הגרעין נובע כי $\sigma|_S = Id|_S$, בפרט $\sigma(a_i) = a_i$ לכל $a_i \in S$.

אבל $L = F(a_1, ..., a_n)$, ולכן שימור קבוצת היוצרים גורר את שימור כל L, כלומר $\sigma = Id$. ■

משפט: (Primitive element theorem) אם $F \leq K$ הרחבת גלואה, אז קיים $a \in K$ כך ש-$K = F(a)$.

דוגמה: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. כי $\sqrt{3} - \sqrt{2} = (\sqrt{2} + \sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. נחבר ונחסר ונקבל את $\sqrt{2}, \sqrt{3}$.

הוכחה: נתון כי ההרחבה סופית, אז נסמן $K = F(a_1, ..., a_n)$ ל-n מזערי. אם $n = 0$ אז $K = F$ ואם $n = 1$ אז $K = F(a_1)$, ולכן סיימנו. אז נניח כי $2 \leq n$.

נשים לב כי $K = F(a_1, ..., a_n) = F(a_1, a_2)(a_3, ..., a_n)$. לכן אם נראה כי $F(a_1, a_2) = F(b)$ ל-$b \in K$ כלשהו נסיים, כי אז נוכל להסיק ש-K נוצר על־ידי $n - 1$ איברים, בסתירה לבחירת n כמזערי, ולכן בהכרח $n \leq 1$.

אם כך יש להוכיח ש-$F(a_1, a_2) = F(b)$ ל-$b \in K$ כלשהו. נחלק לשני מקרים:

- אם F שדה סופי, אז K הוא מרחב וקטורי ממימד n מעליו. לכן $K \cong F^n$ ומכאן כי $|K| = |F|^n$.

  החבורה הכפלית של כל שדה סופי היא ציקלית, ולכן נוכל לסמן $K^* = K \backslash \{0\} = \langle b \rangle$. מכאן כי b הנ"ל יוצר את K כולו.

- אם F שדה אינסופי, נתבונן בקבוצה $\{a_1 + \alpha a_2 | \alpha \in F\}$. באופן כללי מתקיים $F \leq F(a_1 + \alpha a_2) \leq F(a_1, a_2)$ לכל $\alpha \in F$.

  אבל הראינו לעיל שלכל הרחבה סופית של שדה מושלם יש מספר סופי של שדות ביניים, ולכן קיימים $\alpha, \beta \in F$ שונים, כך ש-$F(a_1 + \alpha a_2) = F(a_1 + \beta a_2)$. נסמן שדה זה ב-$K'$ ונראה כי $K = K'$.

---

[45]הראינו עובדה זו בשלב הראשון של הוכחת המשפט המאפיין הרחבות נורמליות.

[46]הרכבת פונקציות היא אסוציאטיבית ואדישה לפעולת הצמצום.

[47]בהמשך נשיג חסם טוב יותר על הגודל של $Aut(L/F)$.

מצד אחד ברור כי $K' \subset K$, כי $a_1, a_2 \in K$ ולכן גם $a_1 + \alpha a_2 \in K$. נראה את ההכלה ההפוכה, שלשם כך יש להראות כי $a_1, a_2 \in K'$. אבל:

$$\begin{cases} a_1 + \alpha a_2 \in K' \\ a_1 + \beta a_2 \in K' \end{cases} \Longrightarrow (\alpha - \beta)\, a_2 \in K' \underset{\substack{\alpha \neq \beta \\ \text{hence} \\ (\alpha-\beta)^{-1} \in K'}}{\Longrightarrow} a_2 \in K'$$

ולכן גם $a_1 = (a_1 + \alpha a_2) - \alpha a_2 \in K'$. ■

מסקנה: הראינו כי $|G| \leq |S|!$, ל-S קבוצת שורשי הפולינום שמתאפס על כל יוצרי K מעל F. לאור המשפט האחרון ניתן לשפר את החסם: $|Aut\left({}^{K}\!/_{F}\right)| \leq [K : F]$.

הוכחה: נסמן $G = Aut\left({}^{K}\!/_{F}\right)$. מהמשפט האחרון נובע שלהרחבה $F \leq K$ קיים יוצר יחיד $K = F(a)$. נגדיר $f = \min p(a)$ הפולינום המינימלי של a מעל F, ונגדיר את S להיות קבוצת כל השורשים שלו.

תזכורת: כל הומומורפיזם בין חבורה לחבורת סימטריות $Sym(1, ..., n)$, ניתן לזהות עם פעולה של החבורה על הקבוצה $\{1, ..., n\}$.

כעת נתבונן בהעתקה $G \to Sym(S)$ המוגדרת על־ידי $\sigma \mapsto \sigma|_S$. ראינו לעיל שזה הומומורפיזם. הפעולה המתאימה להומומורפיזם זה היא פעולת G על הקבוצה S על־ידי $\sigma.b = \sigma(b)$.

המייצב של a מהגדרתו הוא $G_a =: \{\sigma \in G | \sigma(a) = a\}$. נשים לב כי $K = F(a)$ ולכן $G_a = \{Id\}$ בלבד, כי מייצב של קבוצת יוצרים מייצב את השדה כולו.

לכן הגרעין של הפעולה טריוויאלי, ומכאן שההעתקה $G \to S$ המוגדרת $\sigma \mapsto \sigma(a)$, שהיא ההעתקה המתאימה להומומורפיזם, היא חח"ע. מכאן כי $|G| \leq |S|$.

אבל $|S| \leq \deg(f) = [K : F]$, ולכן $|G| \leq [K : F]$. ■

הערה: החסם $|G| \leq [K : F]$ מושג אם ורק אם $F \leq K$ הרחבה נורמלית.

בכיוון ראשון, אם $F \leq K$ הרחבה נורמלית אז $|S| = \deg f$, כי K מכיל את השורש a של f ולכן הוא שדה פיצול של f.

כמו־כן הפעולה $G \to S$, $\sigma \mapsto \sigma(a)$ חח"ע כפי שהראינו בהוכחה. ונשים לב שלכל $a' \in K$ שורש של f קיים $\sigma \in G$ כך ש-$\sigma(a) = a'$, ולכן זו העתקה על S. מכאן שמתקיים $|G| = |S| = \deg f = [K : F]$.

בכיוון שני, אם $F \leq K$ הרחבה שאינה נורמלית, אז מתנאי שקול שהראינו לעיל נובע שקיים אוטומורפיזם $\sigma \in G$ שאינו משמר את K. לכן המייצב שהזכרנו בהוכחה G_a אינו חח"ע, ולכן $|G| \lneqq |S|$.

משפט (חלק ב' של התאמת גלואה): תהי $F \leq L$ הרחבת גלואה, ותהי $H \leq Aut\left({}^{L}\!/_{F}\right)$. נגדיר $K = fix(H)$ ונסמן $H' = Aut\left({}^{L}\!/_{K}\right)$. אזי $H = H'$.

מסקנה: ההתאמה בין תתי החבורות לשדות הביניים $H \mapsto fix(H)$, היא חח"ע.

כי אם H_1, H_2 תתי־חבורות המועתקות לאותו שדה ביניים $F \leq K \leq L$, ניתן להפעיל את ההעתקה ההפוכה ולקבל כי $H_1 = H_2$.

הוכחה: ראשית ברור כי $H \subset H'$, שכן לכל $\sigma \in H$, לכל $a \in K = fix(H)$ כמובן $\sigma(a) = a$, ולכן $\sigma \in H'$.

כדי לקבל את השוויון $H = H'$ מספיק להראות כי $|H| \le [L:K]$. וזאת כי נוכל להסיק $|H| \le |H'| \le [L:K] \le |H|$,[48] ולכן בהכרח $|H| = |H'|$. מכך ששתיהן סופיות ומההכלה $H \subset H'$ נסיק כי $H = H'$.

נראה כי $|H| \le [L:K]$: מ-Primitive element theorem נובע שקיים $a \in L$ כך ש-$L = F(a)$, ובפרט נובע $L = K(a)$. נסמן $f =: \min p(a)$ מעל K.

אם נמצא פולינום $h \in K[x]$ שדרגתו חסומה על־ידי $|H|$ שמאפס את a, נוכל להסיק ש-$[L:K] = [K(a):K] = \deg(f) \le \deg(h) \le |H|$, כאשר אי השוויון השני נובע ממינימליות f ביחס לכל שאר הפולינומים שמאפסים את a.

נגדיר $h(x) = \prod_{\tau \in H} (x - \tau(a))$ ונראה שזה הפולינום המבוקש.

ראשית קל לראות כי $h(a) = 0$, כי $Id \in H$ ולכן $x - a | h$ ב-$L[x]$. כמו־כן $\deg h = |H|$. נותר להראות כי $h \in K[x]$.

נסמן $h(x) = x^n + b_n x^{n-1} + ... + b_0$. צריך להראות כי $b_i \in K = fix(H)$ לכל i. כלומר שלכל $\sigma \in H$ מתקיים $\sigma(b_i) = b_i$.

יהי $\sigma \in H$. כלומר הוא אוטומורפיזם של ההרחבה $F \le L$ ומשמר את F. נרחיב אותו להיות אוטומורפיזם של ההרחבות $F[x] \le L[x]$ על־ידי: $\sigma\left(\sum \alpha_i x^i\right) =: \sum \sigma(\alpha_i) x^i$. כעת נחשב:

$$h(x) = \prod_{\tau \in H} (x - \tau(a))$$

$$\Downarrow$$

$$\sigma(h(x)) = \sigma\left(\prod_{\tau \in H} (x - \tau(a))\right) = \prod_{\tau \in H} (x - \sigma(\tau(a))) = h(x)$$

כאשר השוויון האחרון נובע מכך ש-$\sigma : H \to H$ הוא אוטומורפיזם, ולכן רק מערבב את סדר הגורמים של h. ■

הגדרות: ראינו שלהרחבת גלואה $F \le L$ יש חבורת אוטומורפיזמים $Aut(L/F)$. לפי התאמת גלואה לכל שדה ביניים K מתאימה חבורה יחידה $H = Aut(L/K)$, ומתקיים $K = fix(H)$.

בהוכחת המשפט האחרון הגדרנו פולינום $h(x) = \prod_{\tau \in H} (x - \tau(a))$ ל-$a \in L$ יוצר של L. אמנם מתקיים $\tau(a) \in L$ לכל $\tau \in H$, אולם ראינו שמקדמי הפולינום הזה הם ב-K.

בהינתן זוג של שדה ביניים K ותת־חבורה מתאימה H, למקדמי הפולינום h הנ"ל יש חשיבות מיוחדת.

- להרחבת גלואה $F \le K \le L$, **הנורמה** של הפולינום h עבור $a \in L$ יוצר, מוגדרת ומסומנת $N_{L/K}(a) =: \prod_{\tau \in H} \tau(a)$.
  נשים לב שהמקדם החופשי של h הוא $\pm N_{L/K}(a)$.
- להרחבת גלואה $F \le K \le L$, **העקבה** של הפולינום h עבור $a \in L$ יוצר, מוגדרת ומסומנת $Tr_{L/K}(a) = \sum_{\sigma \in H} \sigma(a)$.

[48] האי־שוויון הראשון נובע מכך ש-$H \subset H'$, והאי־שוויון השני נובע מהחסם המשופר שהשגנו במסקנה מ-Primitive element theorem.

הערה: נשים לב כי $Tr_{L/K}(a) \in fix(H)$ וכן $N_{L/K}(a) \in fix(H)$.

טענה: עבור הרחבת גלואה $F \leq L$ ושדות ביניים K, K' עם תתי החבורות המתאימות גלואה H, H', מתקיים $K \subset K' \iff H' \subset H$.

(ההוכחה מושארת כתרגיל).

מסקנה: יהי F שדה, ונניח כי p בעיה אלגברית מעליו, כלומר p נתונה על ידי מערכת של משוואות אלגבריות מעל F. נניח עוד כי (α_1, α_2) פתרון יחיד ל-p בתוך שדה הרחבה $F \leq K$. אזי $(\alpha_1, \alpha_2) \in F$.

הוכחה: נתבונן בהרחבה הסופית $F \leq F(\alpha_1, \alpha_2)$. ניקח הרחבת גלואה $F(\alpha_1, \alpha_2) \leq L$ כלשהי (הראינו שתמיד קיימת כזאת), ונתבונן בחבורת גלואה המתאימה $G =: Aut(L/F)$. נשים לב שלכל $\sigma \in G$, מהיותו אוטומורפיזם נובע כי $\sigma(\alpha_1, \alpha_2)$ גם פתרון ל-p. אם כך מיחידות הפתרון נסיק $\sigma(\alpha_1, \alpha_2) = (\alpha_1, \alpha_2)$ לכל $\sigma \in G$, כלומר $(\alpha_1, \alpha_2) \in fix(G)$. אבל מתורת גלואה נובע $fix(G) = F$, כלומר $(\alpha_1, \alpha_2) \in F$.
■

11 הקשר בין נורמליות בחבורות ובשדות

תזכורת: **פעולה** של חבורה G על קבוצה X, היא העתקה $G \times X \to X$, כך ש-$(e, x) \mapsto x$ וגם $(gh, x) = (g, (h, x))$ לכל $x \in X$ ולכל $g, h \in G$.

הגדרה: תהי $F \leq L$ הרחבת גלואה ותהי $G = Aut(L/F)$.

נגדיר פעולה של G על אוסף שדות הביניים, על־ידי $\sigma K = \{\sigma(a) | a \in K\} = \sigma(K)$.
קל לראות שזו אכן פעולה.

טענה: יהי K שדה ביניים ותהי $H = Aut(L/K)$ מתאימה לו גלואה. אז החבורה המתאימה גלואה של σK ל-$\sigma \in G$ כלשהו היא $\sigma H \sigma^{-1}$. כלומר $Aut(L/\sigma K) = \sigma H \sigma^{-1}$.

הוכחה: החבורה המתאימה גלואה לשדה הביניים σK מההגדרתה היא $Aut(L/\sigma K)$.

כלומר כל $\tau \in Aut(L/\sigma K)$ צריך לקיים $\tau(\sigma(a)) = \sigma(a)$ לכל $a \in K$. כלומר $\sigma^{-1}(\tau(\sigma(a))) = a$ לכל $a \in K$.

מכאן $\tau \in Aut(L/\sigma K) \Leftrightarrow \sigma^{-1} \circ \tau \circ \sigma = Id|_K$ ולכן $Aut(L/\sigma K) = \sigma H \sigma^{-1}$. ■

מסקנה: תהי $F \leq L$ הרחבת גלואה ויהי $\sigma \in G$. אזי $\sigma K = K \iff \sigma^{-1} H \sigma = H$.

הוכחה: בכיוון ראשון, אם $\sigma K = K$ אז ודאי $\sigma^{-1} H \sigma = Aut(L/\sigma K) = Aut(L/K) = H$.

בכיוון שני, נניח כי $\sigma^{-1} H \sigma = H$, אזי $Aut(L/\sigma K) = Aut(L/K)$.

נפעיל את ההעתקה ההפוכה fix על שני הצדדים ונקבל $\sigma K = K$. ■

מסקנה: תהי $F \leq L$ הרחבת גלואה. אזי תת הרחבה $F \leq K$ היא נורמלית, אם ורק אם החבורה המתאימה לה גלואה $Aut(L/K)$ היא תת־חבורה נורמלית של $Aut(L/F)$

הוכחה: נובע מיד מהמסקנה הקודמת, כשמפעילים אותה לכל $\sigma \in G$. ■

12 חבורת גלואה כבסיס למרחב וקטורי

תזכורת: בהינתן חוג R ומודול M מעל R, אנדומורפיזם של מודולים הוא העתקה $M \to M$ שהיא הומומורפיזם של מודולים, כלומר המשמרת את החיבור ואת הכפל בסקלר.

אוסף האנדומורפיזמים מסומן $Hom_R(M,M)$ או $End_R(M)$.

בפרט במקרה בו לוקחים F שדה ומודול V מעל F, כלומר מרחב וקטורי, מתקיים כי $End_F(V)$ הוא בדיוק אוסף ההעתקות ה-F־לינאריות $V \to V$. או באופן אחר, אוסף המטריצות מסדר $\dim_F(V) \times \dim_F(V)$.

מבוא: תהי $F \le L$ הרחבת גלואה ותהי $G = Aut(L/F)$. נראה בחלק זה כיצד ניתן להתייחס ל-G כאל בסיס של $End_F(L)$, כאשר מתייחסים לזה האחרון כמרחב וקטורי מעל L.

- נשים לב כי $G \subset End_F(L)$, כי לכל $\sigma \in G$, לכל $x,y \in L$ ולכל $\alpha \in F$, מתקיים $\sigma(x+y) = \sigma(x) + \sigma(y)$ וכן $\sigma(\alpha x) = \sigma(\alpha)\sigma(x) = \alpha\sigma(x)$.

  נשים לב שהשתמשנו בכך ש-G משמרת את F, ולכן $\sigma(\alpha) = \alpha$. כלומר כל אוטומורפיזם $\sigma \in G$ הוא העתקה F־לינארית אבל לא L־לינארית.

- נשים לב עוד כי $End_F(L)$ מהווה מרחב וקטורי מעל L. החיבור מוגדר בו באופן טבעי, והכפל בסקלר מוגדר על־ידי $\alpha \cdot h = \alpha \cdot_L h$.[49] כלומר $(\alpha h)(x) = \alpha h(x)$ לכל $x \in L$. קל לבדוק שאכן מתקבל אנדומורפיזם.

  אם כך טבעי לבדוק מהו הממד של $End_F(L)$ כמרחב וקטורי מעל L.

טענה: תהי $F \le L$ הרחבת גלואה, ו-V מרחב וקטורי מעל L. אזי $[L:F] \cdot \dim_L(V) = \dim_F(V)$.

נשים לב שזו הכללה של טענה קודמת ל-V הרחבה סופית של L, שאז $[V:F] = [L:F][V:L]$.

הוכחה: יהי $v_1,...,v_k$ בסיס של V מעל L, ויהי $\alpha_1,...,\alpha_n$ בסיס של L מעל F. אזי האוסף $\left\{\alpha_i v_j \middle| \begin{array}{c} 1 \le j \le k \\ 1 \le i \le n \end{array}\right\}$ מהווה בסיס של V מעל F.

את החישוב שמראה מדוע זה אכן בסיס ניתן לראות בהוכחת הטענה הקודמת.[50] ■

משפט: תהי $F \le L$ הרחבת גלואה ותהי $G = Aut(L/F)$. אז G כתת־קבוצה של $End_F(L)$ היא בלתי תלויה לינארית.

הוכחה: נסמן $|G| = n$. צריך להראות שעבור $\alpha_1,...,\alpha_n \in L$ כלשהם, מתקיים כי אם $\sum_{i=1}^{n} \alpha_i \sigma_i = 0$ אז $\alpha_i = 0$ לכל $1 \le i \le n$.

נשים לב שלפי הגדרת הכפל בסקלר במרחב $End_F(L)$, המשמעות של השוויון הנ"ל היא $\sum_{i=1}^{n} \alpha_i \sigma_i(x) = 0$ לכל $x \in L$.

נוכיח באינדוקציה על n. עבור $n = 1$ הטענה ברורה. נניח את הטענה עבור $n-1$, ונניח בשלילה כי $\sum_{i=1}^{n} \alpha_i \sigma_i(x) = 0$ לכל $x \in L$, ועדיין $\alpha_1 \neq 0$.

---

[49] הסימון $\cdot_L$ הוא לכפל המוגדר ב-L כשדה.

[50] בראשית פרק 5.

בפרט מתקיים לכל $b \in L$ כי:

$$0=\sum_{i=1}^{n}\alpha_i\sigma_i\left(bx\right)=\sum_{i=1}^{n}\alpha_i\sigma_i\left(b\right)\sigma_i\left(x\right) \tag{1}$$

נכפיל את המשוואה $\sum_{i=1}^{n}\alpha_i\sigma_i\left(x\right)=0$ משמאל בסקלר $\sigma_n\left(b\right)$ ונקבל:

$$\sigma_n\left(b\right)\sum_{i=1}^{n}\alpha_i\sigma_i\left(x\right)=\sum_{i=1}^{n}\alpha_i\sigma_n\left(b\right)\sigma_i\left(x\right)=0 \tag{2}$$

אם נחסר $(1)-(2)$ המחובר האחרון יתאפס, ולכן:

$$0=(1)-(2)=\sum_{i=1}^{n}\alpha_i\sigma_i\left(b\right)\sigma_i\left(x\right)-\sum_{i=1}^{n}\alpha_i\sigma_n\left(b\right)\sigma_i\left(x\right)=\sum_{i=1}^{n-1}\alpha_i\left(\sigma_i\left(b\right)-\sigma_n\left(b\right)\right)\sigma_i\left(x\right)$$

נשים לב ששויון זה הוא צירוף לינארי מאורך $n-1$ שמתאפס על ווקטורים מ-G. לכן מהנחת האינדוקציה כל המקדמים שלו 0.

אולם המקדם הראשון אינו יכול להיות 0, כי הנחנו $\alpha_1\neq 0$ וכן $\sigma_1\neq\sigma_n$ מבחירת הווקטורים ב-G, סתירה. ■

מסקנה: תהי $F\leq L$ הרחבת גלואה. נסמן $G=Aut\left({}^{L}/_{F}\right)$. אזי G בסיס של $End_F\left(L\right)$ כמרחב ווקטורי מעל L.

הוכחה: מהיות $F\leq L$ הרחבה נורמלית נובע $n=:[L:F]=|G|$. נסמן $V=End_F\left(L\right)$ ונשים לב כי $\dim_F\left(V\right)=n^2$, שכן הוא איזומורפי למרחב המטריצות $n\times n$ מעל F.

מנוסחה קודמת $[L:F]\cdot\dim_L\left(V\right)=\dim_F\left(V\right)$ נחלץ כי $\dim_L\left(V\right)=n$. הראינו כי G בת"ל, ומכך שגודלה $|G|=n=\dim_L\left(V\right)$ נובע שהיא בסיס. ■

13 הרחבות ציקליות

הגדרה: הרחבה $F\leq L$ נקראת ***הרחבה ציקלית***, אם F הוא שדה מושלם המכיל שורש יחידה n־י פרימיטיבי, וגם חבורת גלואה שלה $G=Aut\left({}^{L}/_{F}\right)$ ציקלית.

משפט: הרחבת גלואה $F\leq L$ מסדר n ל-F המכיל שורש יחידה n־י פרימיטיבי היא הרחבה ציקלית, אם ורק אם קיים $a\in L\backslash F$ עבורו $L=F\left(a\right)$, כך ש-$a^n\in F$.

הוכחה: (כיוון שני תחילה)

אם יש a כנ"ל, אז לכל $\sigma\in G$ מתקיים $\left(\frac{\sigma(a)}{a}\right)^n=\frac{a^n}{a^n}=1$, ולכן $\omega=\frac{\sigma(a)}{a}$ מהווה שורש יחידה n־י. לכן כל σ הוא מהצורה $\sigma\left(a\right)=\omega a$. מכאן כי $G=\langle\sigma\rangle$.

(כיוון ראשון)

למה: קיים $0\neq a\in L$ כך ש-$\frac{\sigma(a)}{a}$ שורש יחידה לכל $\sigma\in G$.

הוכחה: יהי $\omega \in F$ שורש יחידה. לצורך הנוחות נראה כי $\frac{\sigma(a)}{a} = \omega^{-1}$ (גם זה שורש יחידה), כלומר $\omega\sigma(a) = a$ לכל $\sigma \in G$.

נסמן $G = \left\{1, \sigma, ..., \sigma^{n-1}\right\}$. נשים לב כי $T =: \omega\sigma \in End_F(L)$, וכן $T^n = (\omega\sigma)^n = \omega^n\sigma^n = 1 \cdot Id = Id$, לכן $T^n - 1 = 0$.

נפרק את הביטוי $0 = T^n - 1 = (T-1)\left(T^{n-1} + ... + 1\right)$.[51] נשים לב שמתקיים $T^{n-1} + ... + 1 \neq 0$, אחרת נקבל ווקטורים תלויים לינארית ב-G, בסתירה למשפט הקודם. לכן קיים $c \in L$ שעבורו $a =: \left(T^{n-1} + ... + 1\right)(c) \neq 0$. נראה ש-$a$ זה הוא האיבר הנדרש:

$$(T-1)(a) = (T-1)\left(T^{n-1} + ... + 1\right)(c) = (T^n - 1)(c) = 0$$

כאשר השוויון השני הוא הפירוק של $T^n - 1$, והשוויון השלישי נובע מכך ש-$T^n - 1 = 0$ זהותית. מכאן $T(a) = a$, כלומר $\omega\sigma(a) = a$. ■

כעת נראה כי $a^n \in F$ וכי $L = F(a)$.

1. מתורת גלואה נובע $fix\left(Aut\left(L/F\right)\right) = F$, ולכן אם נראה ש-$\tau(a^n) = a^n$ לכל $\tau \in Aut\left(L/F\right)$ נוכל להסיק כי $a^n \in F$.

מההנחה ש-$Aut\left(L/F\right)$ ציקלית, ונניח שנוצרת על־ידי σ, נובע שמספיק להראות כי $\sigma(a^n) = a^n$:

$$\sigma(a) = \omega^{-1}a \implies \sigma(a^n) = \left(\omega^{-1}a\right)^n = a^n$$

2. מתורת גלואה נובע שאם $Aut\left(L/F(a)\right) = \{Id\}$, כלומר שרק אוטומורפיזם הזהות משמר את $F(a)$, אז בהכרח $L = F(a)$. ואכן $\sigma^l(a) = \omega^{-l}a^l \neq a^l$ לכל $1 \leq l < n$ מפרימיטיביות ω. ■

14 פתירות

הגדרה: חבורה G נקראת **פתירה** מסדר n, אם קיים מגדל של תתי־חבורות מהצורה:

$$\{e\} = H_0 \leq H_1 \leq ... \leq H_n = G$$

המקיימות $H_i \lhd H_{i+1}$ לכל $0 \leq i \leq n-1$, וגם H_{i+1}/H_i חבורת מנה אבלית.

הערה: קל לראות שכל חבורה אבלית היא פתירה מסדר 1.

תכונות יסודיות:[52]

1. כל תת־חבורה של חבורה פתירה, היא פתירה.

כי אם G פתירה על־ידי המגדל $\{H_i\}$, אז $K \leq G$ פתירה על־ידי המגדל $\{H_i \cap K\}$.

2. כל חבורת מנה של חבורה פתירה, היא פתירה.

כי אם G פתירה על־ידי המגדל $\{H_i\}$, אז G/N פתירה על־ידי המגדל $\{H_i/N\}$.

---

[51] זה לא גורר מיד $T = 1$, כי בחוג המטריצות יש מחלקי אפס.

[52] ההוכחות המלאות הובאו בקורס קודם - "מבנים אלגבריים 1".

3. תהי $N \lhd G$, אזי G פתירה אם ורק אם $N, {}^{G}/_{N}$ פתירות.

בכיוון ראשון הטענה נובעת משתי הטענות הקודמות.

בכיוון השני הטענה נובעת מכך שאם N פתירה על־ידי המגדל $\{N_i\}_{i=0}^{k}$, ו-${}^{G}/_{N}$ פתירה על־ידי המגדל $\{{}^{G_j}/_{N}\}_{j=0}^{l}$, אז G פתירה על־ידי המגדל:

$$\{e\} = N_0 \lhd N_1 \lhd ... \lhd N_k = N = \left\{e_{G/N}\right\} = G_l \lhd ... \lhd G_0 = G$$

4. אם G אבלית, סופית ופתירה, אז חבורות המנה של המגדל שלה ציקליות מסדר ראשוני.

כי מסופיות G ניתן להגיע לעידון מקסימלי של המגדל, ובמצב זה חבורות המנה הן פשוטות. ידוע שכל חבורה סופית שהיא אבלית ופשוטה, היא ציקלית מסדר ראשוני.

5. תהי $H \leq S_p$ ל-p ראשוני. אם $p \,|\, |H|$,[53] ויש חילוף $(ij) \in H$, אז $H = S_p$.

במילים אחרות: S_p נוצרת על־ידי כל מחזור באורך p עם כל חילוף.

הערה: לצורך ההמשך, כדאי לשים לב שנורמליות אינה תכונה טרנזיטיבית. כלומר גם אם $N_1 \lhd N_2 \lhd G$, לא בהכרח $N_1 \lhd G$.

למשל: ניקח את $D_4 = \langle s, r \rangle$ (r סיבוב של 90° ו-s שיקוף כלשהו). מתקיים $D_4 \rhd \langle r^2, s \rangle \rhd \langle s \rangle$, כי r, s^2 מתחלפים, אבל מצד שני $D_4 \ntriangleright \langle s \rangle$ כי r, s לא מתחלפים.

הגדרה: תהי $F \leq K$ הרחבת גלואה ל-F שדה ממציין אפס. אומרים שזו **הרחבה פתירה**, אם $Aut\left({}^{K}/_{F}\right)$ חבורה פתירה.

לעתים מגדירים פתירות של הרחבה כנ"ל, אם קיימת הרחבה $F \leq K \leq L$, כך ש-$Aut\left({}^{L}/_{F}\right)$ חבורה פתירה. השקילות בין המשמעויות של ההגדרות נובעת מההערה הבאה:

הערה: אם $F \leq L$ הרחבת גלואה פתירה ונתון שדה ביניים K, אז גם $F \leq K$ פתירה.

נשים לב שההעתקה $Aut\left({}^{L}/_{F}\right) \to Aut\left({}^{K}/_{F}\right)$ המוגדרת על־ידי $\sigma \mapsto \sigma|_K$ היא הומומורפיזם של חבורות. זו גם העתקה על (תרגיל), ולכן פתירות החבורה בתחום גוררת את פתירות החבורה בטווח.

14.1 פתירות בעזרת רדיקלים

הגדרה: יהי F שדה ממציין אפס. אומרים שפולינום $f \in F[x]$ **פתיר בעזרת רדיקלים** מעל F, אם קיים מגדל של הרחבות שדות $F = F_0 \leq F_1 \leq ... \leq F_n$, כך ש-$f$ מתפצל ב-F_n, ולכל $0 \leq i \leq n-1$ מתקיים כי $F_{i+1} = F_i(a_i)$, עבור $a_i \in F_{i+1}$ המקיים $a_i^{m_i} \in F_i$ לאיזה $2 \leq m_i$.

סימון: בהינתן $f \in F[x]$ ל-F ממציין אפס, נסמן ב-$L(f, F)$ את שדה הפיצול המזערי של f מעל F. עוד נסמן $Gal(f, F) = Aut\left({}^{L(f,F)}/_{F}\right)$.

[53] נשים לב כי $p \,|\, |H|$ אם ורק אם יש ב-H מחזור מאורך p. בכיוון ראשון הטענה נובעת ממשפט קושי לחבורות, ובכיוון שני הטענה נובעת מכך שסדרו של מחזור מאורך p הוא p, וסדר של איבר מחלק את גודל החבורה.

הערות:

1. $Gal\left(f,F\right) = Aut\left({}^{L(f,F)}/_{F}\right)$ טריוויאלית אם ורק אם $\left[L\left(f,F\right):F\right]=1$ אם ורק אם $L\left(f,F\right)=F$ אם ורק אם f מתפצל ב-F.
2. בהינתן הרחבה כלשהי $F\le K$ קל לראות כי $L\left(f,F\right)\subset L\left(f,K\right)$, כי $L\left(f,F\right)$ נוצר על־ידי שורשי f מעל F ו-$L\left(f,K\right)$ חייב להכיל אותם כדי להיות שדה פיצול.

   כמו כן מתקיים כי $F\le L\left(f,F\right)$, $K\le L\left(f,K\right)$ הרחבות נורמליות, מהיות השדות הגדולים שדות פיצול מזעריים.

   נתבונן בהומומורפיזם הצמצום $Gal\left(f,K\right)\to Gal\left(f,F\right)$. נראה בהמשך שהוא חח"ע ולכן מתקבל גם היחס $Gal\left(f,K\right)\le Gal\left(f,F\right)$.

הגדרה: יהי F שדה ממציין אפס ותהי $F\le K$ הרחבת גלואה. אומרים כי $F\le K$ **הרחבה רדיקלית**, אם קיים מגדל של תתי שדות מהצורה:

$$F=K_0\le K_1\le ...\le K_r=L$$

כך שכל K_{i+1} מתקבל מ-K_i על ידי סיפוח **רדיקל** כלשהו. כלומר, לכל $0\le i\le r-1$ קיים $a_i\in K_{i+1}$ המקיים $K_{i+1}=K_i\left(a_i\right)$, וכן $a_i^{l_i}\in K_i$ לאיזה $2\le l_i$.

משפט: תהי $F\le K$ הרחבת גלואה מסדר המחלק n כלשהו, עבור F שדה ממציין אפס המכיל שורש יחידה n־י פרימיטיבי.

אם $G=Aut\left({}^{K}/_{F}\right)$ חבורה פתירה, אזי $F\le K$ הרחבה רדיקלית, כל הרחבת ביניים היא נורמלית, ואם נסמן דרגת כל הרחבת ביניים ב-l_i אז $n|l_1\cdot ...\cdot l_r$.

הוכחה: G פתירה וסופית, ולכן קיים מגדל מהצורה $\{e\}=H_0\lhd H_1\lhd ...\lhd H_r=G$, כאשר ${}^{H_{i+1}}/_{H_i}$ ציקלית לכל $0\le i\le r-1$.

נסמן $H^i=H_{r-i}$ ונגדיר $K_i=fix\left(H^i\right)$. נקבל מגדל של תתי שדות $F=K_0\le K_1\le ...\le K_r=K$.

הראינו באופן כללי עבור $H=Aut\left({}^{K}/_{F}\right),\ G=Aut\left({}^{L}/_{K}\right)$ שמתקיים $F\le K$ הרחבה נורמלית $\iff H\lhd G$, ולכן אצלינו מהיות $H^i\lhd H^{i+1}$ נובע כי $K_i\le K_{i+1}$ הרחבה נורמלית.

נשים לב כי מתקיים לחבורת גלואה $Aut\left({}^{K_{i+1}}/_{K_i}\right)={}^{H^{i+1}}/_{H^i}$, ולכן היא ציקלית.
מהמשפט המרכזי שהראינו לעיל לציקליות, נובע שזה תנאי שקול לרדיקליות. ■

הכללה: עבור הרחבת גלואה סופית $F\le K$ מסדר n וכן $G=Aut\left({}^{K}/_{G}\right)$ פתירה, גם אם F <u>אינו</u> מכיל שורש יחידה n־י פרימיטיבי, קיים מגדל תתי שדות הבנוי בעזרת רדיקלים מהצורה $F=K_0\le K_1=F\left(\omega\right)\le ...\le K_r=K\left(\omega\right)$, כאשר ω הוא שורש יחידה n־י פרימיטיבי.

הוכחה: נתבונן ב-$\overline{G}=Aut\left({}^{K(\omega)}/_{F(\omega)}\right)$. נראה כי $\overline{G}$ איזומורפית לתת חבורה של G.

נראה שניתן להפעיל את המשפט הקודם על ההרחבה $F\le K\left(\omega\right)$. ראשית זו הרחבה נורמלית כי אם K הוא שדה הפיצול המזערי של $g\left(x\right)\in F\left[x\right]$ כלשהו, אז $K\left(\omega\right)$ הוא שדה הפיצול המזערי של $g\left(x\right)\left(x^n-1\right)$.[54]

[54] צריך לשים לב שהשתמשנו בכך ש-$x^n-1\in F\left[x\right]$. באופן כללי תיתכן הרחבה $F\le K\le L$, כך ש-$F\le K$ הרחבה נורמלית וגם $K\le L$ הרחבה נורמלית, אבל $K\le L$ אינה נורמלית.

נגדיר העתקה $\rho:\overline{G}\to G$ על ידי הומומורפיזם הצמצום $\sigma\mapsto\sigma|_K$. נשים לב כי $\sigma\in\ker(\rho)$ אומרת ש-σ משמר את $K(\omega)$ כולו ולכן $\sigma=Id$. מכאן ש-ρ חח"ע ולכן $\rho\left(\overline{G}\right)\leq G$. מפתירות G נסיק לפיכך שגם $\overline{G}$ פתירה.

נשים לב עוד כי $\left|K(\omega):F(\omega)\right|=\left|\overline{G}\right|\,|n$. לכן אנו עומדים בתנאי המשפט הקודם, וקיים מגדל $F\leq K_0=F(\omega)=K_1\leq...\leq K_r=K(\omega)$. ■

משפט: תהי $F\leq K$ הרחבה r־רדיקלית, כלומר מתקבלת על ידי סיפוח r רדיקלים, עבור F שדה ממציין אפס.

אזי לכל m טבעי קיימת הרחבה נורמלית ופתירה $F\leq L$ המכילה את K ומכילה גם שורש יחידה m־י פרימיטיבי.

מסקנה: בפרט נובע שלהרחבה רדיקלית $F\leq K$ עבור F שדה ממציין אפס, קיימת הרחבה נורמלית ופתירה $F\leq L$ המכילה את K.

מסקנה יסודית: פולינום $f\in F[x]$ עבור F שדה ממציין אפס ניתן לפתרון על ידי רדיקלים, אם ורק אם קיימת הרחבה נורמלית ופתירה $F\leq K$ בה f מתפצל.

באופן שקול: פולינום אי פריק $f\in F[x]$ עבור F שדה ממציין אפס ניתן לפתרון על ידי רדיקלים, אם ורק אם קיימת הרחבה נורמלית ופתירה $F\leq K$ בה ל-f יש שורש.

הוכחת המסקנה: בכיוון ראשון: אם f כנ"ל ניתן לפתרון בעזרת רדיקלים, כלומר יש הרחבה רדיקלית $F\leq K$ שבה f מתפצל, אז מהמשפט האחרון נובע שקיימת הרחבה נורמלית ופתירה $F\leq L$ המכילה את K, ולכן $Gal(f,F)$ פתירה.

בכיוון שני: נניח שקיימת הרחבה נורמלית ופתירה $F\leq K$ שבה f מתפצל, אז הטענה נובעת מהכללת המשפט שלפני האחרון. ■

הוכחת המשפט: לצורך הוכחת המשפט נוכיח תחילה טענת עזר.

למה: יהי F שדה ממציין אפס המכיל שורש יחידה n־י פרימיטיבי.
יהי $K=F(b_1,...,b_k)$ כשכל b_i רדיקל n־י. כלומר $b_i^n\in F$.
אזי $F\leq K$ הרחבה נורמלית ואבלית. כלומר חבורת גלואה שלה $G=:$ $Aut\left({}^{K}/_{F}\right)$ אבלית.

הוכחת הלמה: נסמן $\mu=\{x\in F^*|x^n=1\}\leq F^*$, תת־חבורה ציקלית מסדר n.
נראה כי G איזומורפית לתת חבורה של $\mu^k=\underbrace{\mu\times...\times\mu}_{k}$. מהיות μ ציקלית נובע כי μ^k אבלית, ומכך נסיק שגם G אבלית.
אם כך נגדיר העתקה $\rho:G\to\mu^k$ על ידי $\rho=(\rho_1,...,\rho_k)$, כאשר $\rho_i:G\to\mu$ ניתנת על ידי $\rho_i(\sigma)=\frac{\sigma(b_i)}{b_i}$. נשים לב שאכן $1=\frac{b_i^n}{b_i^n}=\frac{\sigma(b_i^n)}{b_i^n}=\left(\frac{\sigma(b_i)}{b_i}\right)^n$, כי $b_i^n\in F$ וכל $\sigma\in G$ משמר את F.
נראה שזה הומומורפיזם בכל קואורדינטה ומכך ינבע שזה הומומורפיזם. בהינתן $\sigma,\tau\in G$, נסמן $\rho_i(\sigma)=\frac{\sigma(b_i)}{b_i}=\alpha,\ \rho_i(\tau)=\frac{\tau(b_i)}{b_i}=\beta$. נחשב:

$$\sigma(\tau(b_i))=\sigma(\beta b_i)=\sigma(\beta)\sigma(b_i)=\sigma(\beta)\alpha b_i=\beta\alpha b_i$$

כאשר השוויון $\sigma(\beta)=\beta$ נובע מכך ש-$\beta\in F$. מכאן נובע:

$$\rho_i(\sigma\circ\tau)=\frac{\sigma(\tau(b_i))}{b_i}=\beta\alpha=\rho_i(\sigma)\rho_i(\tau)$$

נותר להראות כי ρ חח"ע. נשים לב כי:

$$\sigma\in\ker\rho\iff\forall_{1\le i\le k}\rho_i(\sigma)=1\iff\forall_{1\le i\le k}\frac{\sigma(b_i)}{b_i}=1\iff\forall_{1\le i\le k}\sigma(b_i)=b_i$$

אבל $b_1,...,b_k$ יוצרים את K מעל F, ולכן $\sigma\in G$ משמר אותם אם ורק אם $\sigma=Id$. מכאן כי $\ker\rho=\{Id\}$ ולכן היא חח"ע. ■

כעת נוכיח את המשפט באינדוקציה על r. אם $r=0$ אז $K=F$. אם כן ניקח את L להיות שדה הפיצול המזערי של $x^m-1\in F[x]$. לכן L מכיל שורש יחידה m־י פרימיטיבי, וכמו כן $Aut\left({}^{L}/_{F}\right)$ חבורה ציקלית.[55]

נניח את הטענה ל-$r-1$ ותהי $F\le K$ הרחבה r־רדיקלית. כלומר קיים $K'\le K$ כך ש-$K=K'(b)$ עבור $b^l\in K'$. בפרט גם ההרחבה $F\le K'$ היא $r-1$־רדיקלית.

- תחילה נראה קיום של שורש יחידה m־י פרימיטיבי: נסמן $m'=m\cdot l$. מהנחת האינדוקציה יש הרחבה נורמלית ופתירה $F\le L'$ המכילה שורש יחידה פרימיטיבי m'־י, ושמכילה את K'.

  נגדיר את הפולינום $f(x)=\prod_{\sigma\in Aut\left({}^{L'}/_{F}\right)}\left(x^l-\sigma\left(b^l\right)\right)\in L'[x]$. נשים לב שלמעשה $f\in F[x]$, שכן כל $\sigma\in Aut\left({}^{L'}/_{F}\right)$ משמר את F ולכן $f\in fix\left(Aut\left({}^{L'}/_{F}\right)\right)[x]=F[x]$, כאשר השוויון האחרון נובע מהתאמת גלואה.

  אם כך יהי L שדה הפיצול המזערי של f מעל L'. מכך ש-$f\in F[x]$ נובע כי $F\le L$ הרחבה נורמלית.[56] אבל הנחנו $L'\le L$ ו-L' מכיל שורש יחידה $m'=m\cdot l$־י פרימיטיבי, ולכן גם שורש יחידה m־י פרימיטיבי.

- כעת נראה שהחבורה $Aut\left({}^{L}/_{F}\right)$ פתירה: מהלמה שהראינו נובע כי $Aut\left({}^{L}/_{L'}\right)$ חבורה אבלית, שכן $L'\le L$ הרחבה רדיקלית, ולכן זו חבורה פתירה.

  נשים לב כי $Aut\left({}^{L}/_{L'}\right)\le Aut\left({}^{L}/_{F}\right)$, וזו גם תת חבורה נורמלית כי $L\le L'$ הרחבה נורמלית. הראינו כי $Aut\left({}^{L'}/_{F}\right)\cong{}^{Aut\left({}^{L}/_{F}\right)}/_{Aut\left({}^{L}/_{L'}\right)}$, ולכן מפתירות $Aut\left({}^{L'}/_{F}\right)$ נובע שגם חבורת המנה פתירה. אבל מהלמה $Aut\left({}^{L}/_{L'}\right)$ אבלית ולכן $Aut\left({}^{L}/_{F}\right)$ פתירה. ■

דוגמה: נראה כיצד למצוא פולינום מדרגה 5 שאינו פתיר בעזרת רדיקלים.

יהי $f\in\mathbb{Q}[x]$ פולינום אי פריק כלשהו ב-$\mathbb{Q}$ מדרגה 5. נניח כי L שדה הפיצול המזערי שלו, ונסמן $G=Aut\left({}^{L}/_{F}\right)$.

מכיוון של-f יש בדיוק 5 שורשים ב-L נובע כי $G\hookrightarrow Sym(5)$, שכן אם $\alpha_1,...,\alpha_5$ שורשי f ב-L אז G פועלת עליהם כתת חבורת תמורות כלשהי.

נשים לב שמצד אחד $[L:\mathbb{Q}]=|G|\,|5!$ כי זו $G\le Sym(5)$, ומצד שני $5|\,[L:\mathbb{Q}]=|G|$, כי עבור ההרחבה $\mathbb{Q}\le\mathbb{Q}(\alpha_1)\le L$ מתקיים $[\mathbb{Q}(\alpha_1):\mathbb{Q}]=5$ כי f אי פריק מדרגה 5.

ממשפט קושי לחבורות מכיוון ש-$5|\,[G]$ נובע שיש ב-G איבר מסדר 5, כלומר מחזור מאורך 5. מכאן שאם G מכילה חילוף כלשהו אז $G=Sym(5)$,[57] וכידוע זו חבורה שאינה פתירה.

---

[55]הטענה מושארת כתרגיל: להוכיח שעבור F שדה ממציין אפס המכיל שורש יחידה m־י, עבור K שדה הפיצול המזערי של $x^m-a\in F[x]$ חבורת גלואה $Aut\left({}^{K}/_{F}\right)$ היא ציקלית.

[56]בהתאם לתנאי שקול לנורמליות שהראינו לעיל.

[57]תרגיל: לכל p ראשוני, מחזור באורך p וחילוף כלשהו (כלומר מחזור מאורך 2) יוצרים את $Sym(p)$.

נשים לב שאם ל-f יש בדיוק שני שורשים מרוכבים, אז הומומורפיזם ההצמדה המרוכבת מחליף בין שני השורשים המרוכבים, כלומר הוא מכיל חילוף כלשהו, ובמקרה זה אכן $G = Sym\left(5\right)$.

חקירת הפולינום $x^5 - 4x + 2$ מעלה שזה אכן המצב לגביו. כלומר פולינום זה אינו פתיר בעזרת רדיקלים.

14.1.1 השדה הנוצר של הפולינומים הסימטריים היסודיים

תזכורת: יהי $\mathbb{Q}\left[t_1, ..., t_n\right]$ חוג הפולינומים ב-n משתנים. שדה השברים של חוג זה הוא שדה הפונקציות הרציונליות $\mathbb{Q}\left(t_1, ..., t_n\right)$, שהוא ממציין אפס.

הגדרה: באופן טבעי $Sym\left(n\right)$ היא חבורה פועלת על $\left\{t_1, ..., t_n\right\}$. נגדיר לפיכך פעולה של $Sym\left(n\right)$ על $\mathbb{Q}\left(t_1, ..., t_n\right)$ על ידי חילוף המשתנים בפונקציה.

למשל עבור $\sigma = \left(12\right) \in Sym\left(n\right)$ יתקיים $\sigma.\left(\frac{t_1}{t_2+t_3}\right) = \frac{t_2}{t_1+t_3}$.

הגדרה: נשים לב שהאיברים הבאים מתוך $\mathbb{Q}\left(t_1, ..., t_n\right)$ שייכים לשדה השבת של $Sym\left(n\right)$:

$$s_1 =: t_1 + ... + t_n = \sum_{i=1}^{n} t_i$$

$$s_2 =: \sum_{i=2}^{n} t_1 t_i + \sum_{i=3}^{n} t_2 t_i + ... + t_{n-1} t_n$$

$$\vdots$$

$$s_n =: t_1 \cdot t_2 \cdot ... \cdot t_n = \prod_{i=1}^{n} t_i$$

כלומר בפעולת $Sym\left(n\right)$ על $\mathbb{Q}\left(t_1, ..., t_n\right)$, הפולינומים הללו, שמכונים **הפולינומים הסימטריים היסודיים**, אינם משתנים תחת אף תמורה.

משפט: $fix\left(Sym\left(n\right)\right) = \mathbb{Q}\left(s_1, ..., s_n\right)$

הוכחה: נסמן $L = \mathbb{Q}\left(t_1, ..., t_n\right),\ K = fix\left(Sym\left(n\right)\right),\ F = \mathbb{Q}\left(s_1, ..., s_n\right)$.

קל לראות כי $F \leq K \leq L$, נרצה להראות כי $F = K$. מהתאמת גלואה נובע שדי להראות כי $Aut\left(L/K\right) = Aut\left(L/F\right)$, שכן הפעלת ההעתקה fix על שני הצדדים תיתן לנו את השוויון המבוקש במשפט. אז נראה ששתי החבורות הללו שוות ל-$Sym\left(n\right)$.

למה: הפולינום $f\left(x\right) = \prod_{i=1}^{n}\left(x - t_i\right)$ שמוגדר לכאורה ב-$L\left[x\right]$, הוא למעשה ב-$F\left[x\right]$.[58]

הוכחה: אם נכתוב את הפולינום במפורש, נקבל:

$$f\left(x\right) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + ... + \left(-1\right)^n s_n$$

ולכן ודאי כל המקדמים ב-$F = \mathbb{Q}\left(s_1, ..., s_n\right)$. ■

[58] כדאי לשים לב שהיצורים הללו הם שדות פולינומים של שדות פונקציות רציונליות.

מהלמה נובע כי L הוא שדה הפיצול המזערי של $f \in F[x]$ שדרגתו n, ולכן $[L:F]|n!$. מצד שני $L \leq fix(Sym(n))$ ולכן מהתאמת גלואה $Sym(n) \leq Aut(L/F)$. לכן $|Aut(L/F)| \, | \, n!$. באופן כללי $|Aut(L/F)| \leq [L:F]$ ולכן בהכרח $Aut(L/F) = Sym(n)$.

אם כך $Aut(L/K) \leq Aut(L/F) = Sym(n)$, אבל $L \leq fix(Sym(n))$ ולכן מהתאמת גלואה גם $Sym(n) \leq Aut(L/K)$, ולכן יש שוויון. ■