מבנים אלגבריים 2

11 ביולי 2011

מרצה: צחיק גלנדר

הערה 0.1 בדר"כ אני מנסה לערוך את הסיכומים שלי כך שהם למעשה "מחברת מוקלדת", כלומר, שומרת על סדר הלימוד בכיתה לפי תאריכים, וכו'.

השנה צחיק לא היה בחלק מהשיעורים ולכן היו "קפיצות" מנושא לנושא. עקב כך, ניסיתי הפעם כמיטה יכולתי לסדר את הסיכום לפי נושאים, ולא לפי תאריכים. עדיין, ניסיתי לציין את התאריכים מהם הגיע החומר.

תוכן עניינים

1 על חוגים

15/2/2011 פרק זה מכיל חומרים ממבנים וחומר נוסף.

הגדרה 1.1 חוג הוא קבוצה R עם שתי פעולות המסומנות ב־$+$ ו־$\cdot$, כאשר:

- $(R,+)$ היא חבורה אבלית.
- הכפל הוא אסוציאטיבי.
- מתקיימת דיסטריביוטיביות:

$$\forall a,b,c\in R\ a\left(b+c\right)=ab+ac,\ \ \left(b+c\right)a=ba+ca$$

חוג יקרא קומוטטיבי אם לכל $a,b\in R$, $ab=ba$.

הערה 1.2 אנו נדון בעיקר בחוגים קומוטטיביים.

הגדרה 1.3 מחלק אפס הוא איבר השונה מאפס $a\in R$ כך שיש $0\neq b$ עבורו $ab=0$.

הגדרה 1.4 תחום שלמות הוא חוג קומוטטיבי ללא מחלקי אפס.

הגדרה 1.5 אם $a=bc$ אז אומרים כי b מחלק את a, ורושמים $b|a$.

הגדרה 1.6 אם A חוג קומוטטיבי עם יחידה 1, איבר a נקרא הפיך אם יש $b\in A$ כך ש־$ab=1$.

מעתה ננית כי A הוא תחום שלמות עם יחידה, אלא אם כן יצויין אחרת.

הגדרה 1.7 איבר $a\in A$ לא הפיך יקרא פריק אם יש $b,c\in A$ לא הפיכים עבורם $a=bc$. אחרת, a נקרא אי פריק.

הגדרה 1.8 איבר $a\in A$ יקרא ראשוני אם $a|bc$ אזי $a|b$ או $a|c$.

תרגיל: איבר ראשוני הוא אי פריק בתחום שלמות A.

הגדרה 1.9 תחום שלמות נקרא תחום פריקות (או תחום פריקות חד ערכית) אם כל איבר ניתן לכתיבה ב"צורה יחידה"[1] כמכפלה של מספר סופי של איברים אי פריקים.

הגדרה 1.10 אידאל I בחוג קומוטטיבי A הוא תת חוג המקיים $I\cdot A\subseteq I$. במקרה זה נסמן $A\triangleright I$.

במקרה זה, נגדיר את חוג המנה להיות:

$$A/I=\{a+I|a\in A\}$$

[1] כלומר, אם $a_1\cdot\ldots\cdot a_n=b_1\cdot\ldots\cdot b_m$ כאשר a_i,b_i אי פריקים (לא הפיכים), אזי $n=m$, ועד כדי שינוי סדר $a_i=b_i\cdot c_i$ עבור איזשהוא c_i הפיך. או, במידה ולמדתם זאת במבנים 1 ־ עד כדי ידידות.

כאשר פעולת החיבור בחוג זה מוגדרת להיות:אזי

$$(a+I)+(b+I)=(a+b)+I$$

ופעולת הכפל היא:

$$(a+I)(b+I)=ab+I$$

הגדרה 1.11 אידאל I בחוג A נקרא אידאל ראשי אם קיים $a\in A$ כך ש:

$$I=(a)=\{ab|b\in A\}$$

תחום ראשי (או תחום אידאל ראשי) הוא תחום בו כל אידאל הוא אידאל ראשי.

הגדרה 1.12 תחום נקרא אוקלידי אם קיימת פונקציה $f:A\backslash\{0\}\to\mathbb{R}^+$ כך שלכל $a,b\in A$:

- קיימים $r,c\in\mathbb{R}^+$ כך ש־$b=ac+r$ המקיימים $f(r)<f(a)$ או $r=0$.
- $f(ab)\geq f(a)$.

הגדרה 1.13 בהנתן $a,b\in A$, c יקרא gcd של a ו־b, ונסמן $c=(a,b)$ אם $c|a$, $c|b$, ולכל d המקיים $d|a$ וכן $d|b$ אזי $d|c$.

דוגמאות לחוגים אוקלידיים:

- $\mathbb{Z}$.
- $\mathbb{F}[x]$ חוג פולינומים מעל שדה.

בתחום אוקלידי לכל a,b יש gcd - זוהי מסקנה מאלגוריתם אוקלידס למציאת gcd.

הגדרה 1.14 עבור חוג קומוטטיבי A:

- $I\triangleleft A$ נקרא ראשוני אם $a\cdot b\in I$ אז $a\in I$ או $b\in I$.
- $I\triangleleft A$ נקרא מקסימלי אם אין אידאל ממש המכיל אותו.

תזכורת: I ראשוני $\Leftrightarrow$ A/I תחום שלמות.
I מקסימלי $\Leftrightarrow$ A/I שדה, ובפרט מקסימלי הוא ראשוני.

למה 1.15 A הוא תחום פריקות אמ"מ כל איבר אי פריק הוא ראשוני, וכל שרשרת עולה של אידאלים ראשיים מתייצבת.

21/2/2011

הגדרה 1.16 תחום נקרא נטרי אם כל אידאל הוא נוצר סופית.

למה 1.17 חוג R הוא נטרי אמ"מ כל שרשרת עולה של אידאלים מתייצבת.

הוכחה: $\Leftarrow$ אם R נטרי, תהי $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ שרשרת עולה של אידאלים. נגדיר את אידאל האיחוד שלהם להיות $I = \bigcup_{i=1}^{\infty} I$. ראינו במבנים 1 כי זהו אכן אידאל.

R נטרי, לכן I נוצר סופית. נניח $I = \langle a_1, ..., a_k \rangle$. נגדיר אינדקסים חדשים n_i כך שלכל $1 \leq i \leq k$, $a_i \in I_{n_i}$. יהי $n = \max_{1 \leq i \leq n} n_i$. אזי $a_1, ..., a_k \subseteq I_n$. נקבל:

$$I = \langle a_1, ..., a_k \rangle \subseteq I_n \subseteq I$$

כאשר ההכלה השמאלית נובעת מכך ש־I_n מכיל את היוצרים של I ולכן, מתכונות האידאל, בפרט מכיל את I, וההכלה הימנית נובעת מכך ש־I_n הוא אידאל בשרשרת, ולכן בפרט מוכל באיחוד של כל האידאלים בשרשרת בזו.

לכן השרשרת מתייצבת, כפי שרצינו להראות.

$\Rightarrow$ את הכיוון השני נוכיח בדרך שונה מהמצופה ־ נראה כי אם R אינו נטרי, השרשרת אינה מתייצבת.

אם כך, נניח כי R אינו נטרי, כלומר קיים $I \lhd R$ אידאל שאינו נוצר סופית. נבחר $0 \neq a_1 \in I$, ונגדיר סדרה a_n בצורה רקורסיבית ע"י כך שבכל שלב נבחר $a_i \in I \setminus \langle a_1, ..., a_{i-1} \rangle$. נשתמש בסדרה זו על מנת להגדיר סדרה של אידאלים בצורה הבאה:

$$\forall n \in \mathbb{N}\ I_n = \langle a_1, ..., a_{n-1} \rangle$$

אזי, מההגדרה של הסדרה, I_n היא סדרה עולה ממש של אידאלים:

$$I_1 \subsetneq I_2 \subsetneq ...$$

שאינה מתייצבת (מכיוון ו־I אינו נוצר סופית, נוכל בכל שלב למצוא a_n מתאים). ■

למה 1.18 יהא R תחום ראשי. אזי:

1. R נטרי.
2. עבור $a \in R$ התנאים הבאים שקולים:
   (א) a אי פריק.
   (ב) a ראשוני.
   (ג) האידאל הנוצר על ידי a הוא מקסימלי.

הוכחה: 1 ברור, כי לפי ההגדרה של תחום ראשי, כל אידאל נוצר על ידי איבר אחד, ולכן לבטח כל אידאל נוצר סופית.

נוכיח את 2 ־ נשים ♡ כי הגרירות ג'←ב'←א' תמיד מתקיימות עבור כל חוג קומוטטיבי עם יחידה ־ ראינו זאת במבנים 1.

כלומר, בכל חוג a ראשוני הוא אי פריק, וכן a ראשוני אמ"מ (a) ראשוני (מההגדרה) אמ"מ $R/(a)$ תחום שלמות. כמו כן ראינו כי $R/(a)$ שדה אמ"מ (a) מקסימלי $\Leftarrow$ (a) ראשוני. ברור כי שדה הוא תחום שלמות.

למעשה, הגרירה היחידה שאינה טריוואלית (או שלא הוכחנו במבנים 1) היא שאם a אי פריק אזי (a) מקסימלי.

יהי a אי פריק, ונניח בשלילה כי (a) אינו מקסימלי, כלומר קיים $I \lhd R$ כך ש: $(a) \subsetneq I \subsetneq R$. R תחום ראשי, ולכן קיים $b \in R$ עבורו $(b) = I$. כמו כן $a \in (a) \subseteq I$, לכן קיים

c כך ש־$a = b \cdot c$. אבל a אי פריק, לכן c הפיך, ולכן $(a) = (b) = I$ בסתירה לכך ש־(a) אינו מקסימלי. ■

כעת נוכיח את החלק השני של המשפט מהשיעור הקודם, בעזרת המשפט הבא:

משפט 1.19 אם R תחום נטרי בו כל אי פריק הוא ראשוני, אזי R הוא תחום פריקות.

הערה 1.20 זה מוכיח את המשפט "תחום ראשי הוא תחום פריקות", כי מהחלק הראשון של הלמה מעלה תחום ראשי הוא נטרי, וכן מהשקילות בחלק השני של הלמה נקבל כי בתחוום ראשי כל אי פריק הוא ראשוני.

נוכיח אם כך את המשפט מעלה: **הוכחה: קיום פריקות:**
יהא $a \in R$ כלשהוא, וצריך להוכיח כי a ניתן לפירוק למכפלה של אי פריקים.
אם a אי פריק בעצמו סיימנו. אחרת, קיים a_1 המחלק ממש את a, כלומר $a_1|a$. אם a_1 אי פריק אזי קיים b_1 כך ש: $a = a_1 \cdot b_1$[2]. אחרת, קיים $a_2|a_1$ ממש. אם a_2 אי פריק, נרשום $a = a_2 \cdot b'$, אחרת קיים $a_3|a_2$ ממש, וכן הלאה...
כך נקבל שרשרת עולה של אידאלים $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq ...$. R נטרי, לכן השרשרת הנ"ל מתייצבת בשלב מסויים ־ נניח כי היא מתייצבת בשלב ה־n ־ כלומר, a_n אי פריק. נסמן $a_n = \alpha_1$.

מסקנה 1.21 אם a פריק, אזי יש α_1 אי פריק כך ש־$a = \alpha_1 \cdot b_2$. אם b_2 אי פריק, סיימנו. אחרת, קיים $\alpha_2|b_2$ כך ש־$a = \alpha_1 \cdot \alpha_2 \cdot b_3$, כאשר α_1, α_2 אי פריקים. ואז שוב ־ אם b_3 אי פריק סיימנו, אחרת קיים α_3 ו־b_4, וכו'...

סדרת האידאלים $(b_1) \subsetneq (b_2) \subsetneq ...$ מתייצבת מהנטריות של R, נניח בשלב ה־m. לכן ניתן לרשום $a = \alpha_1 \cdot \alpha_2 \cdot .... \cdot \alpha_{m-1} \cdot \alpha_m$ מכפלה של אי פריקים, כנדרש.
יחידות:
נניח $\alpha_n \cdot ... \cdot \alpha_1 = a = \beta_1 \cdot ... \cdot \beta_m$ מכפלות של אי פריקים. עלינו להראות כי עד כדי שינוי סדר ומכפלה בהפיכים, $\alpha_i = \beta_i \cdot \nu_i$ כאשר ν_i הפיך, וכן $m = n$.
α_1 אי פריק, ועל כן ראשוני. $\alpha_1|a = \beta_1 \cdot ... \cdot \beta_m$, ולכן, או ש־$\alpha_1|\beta_1$, או ש־$\alpha_1|\beta_2 \cdot ... \cdot \beta_m$. אם האפשרות הראשונה נכונה, אזי $\alpha_1 = \beta_1 \cdot \nu_1$ כאשר ν_1 הפיך, אחרת האפשרות השניה נכונה, לכן או ש־$\alpha_1|\beta_2$ או ש־$\alpha_1|\beta_3 \cdot ... \cdot \beta_m$. אם האפשרות הראשונה נכונה, אזי $\alpha_1 = \beta_2 \cdot \nu_2$ כאשר ν_2 הפיך, אחרת ־ כמו קודם.
בדרך זו ניתן להראות כי $\alpha_1 = \beta_i \cdot \nu_i$ עבור i כלשהוא, כאשר ν_i הפיך, וכך עבור כל α_j, כאשר $2 \leq j \leq n$.
מדוע $m = n$? לא עשינו בכיתה, אבל אם מצאנו התאמה כלמעלה, למעשה התאמנו כל איבר α_i בדיוק לβ_i אחד. התהליך סימטרי, כך שגם ל־β_i ניתן להתאים באותה הצורה בדיוק את אותו α_i כך נקבל התאמה חח"ע ועל ־ ולכן גודל הקבוצות זהה, כלומר, $m = n$.
נציין כי אם קיימות כפילויות, כלומר אם קיימים $\alpha_i = \alpha_j,\ i \neq j$, במידה והותאמו לאותו ה־$\beta_i$, בתהליך הסימטרי נקבל כי יש $\beta_i = \beta_j,\ i \neq j$, ולכן נוכל להגדיר התאמה חח"ע ועל ללא בעיה, כנדרש. ■

מסקנה 1.22 אם $\mathbb{F}$ הוא שדה, אזי חוג הפולינומים מעל השדה ־ $\mathbb{F}[x]$ הוא חוג אוקלידי, ובפרט ראשי, ובפרט הוא חוג פריקות (כאשר הפונקציה היא המעלה של הפולינום לתוך $\mathbb{R}^+$).

[2] לא להבהל, כעת אנחנו לא מתייחסים ל־bאים, אבל בהמשך נטפל גם בהם באותה הצורה.

בחוג זה נתעניין במסגרת הקורס, וזהו המושג המרכזי בתורת גלואה (ובהתחלה של תורת השדות).

הערה 1.23 נשים ♡ כי הכיוון השני של הטענה אינו נכון! נראה זו בהמשך העזרת הלמה של גאוס.

22/2/2011

הערה 1.24 gcd עבור כל $a,b\in R$ מוגדר היטב כאשר R תחום פריקות.

הגדרה 1.25 אם $f\in R\left[x\right]$, ונסמן $f=a_nx^n+...+a_0$, נאמר ש־f פרימיטיבי אם ה־gcd של מקדמיו הוא 1.

למה 1.26 יהא R תחום פריקות עם יחידה, ויהיו $f,g\in R\left[x\right]$ פולינומים פרימיטיביים. אזי המכפלה של $f\cdot g$ היא גם פולינום פרימיטיבי.

הוכחה: נניח בשלילה כי $f\cdot g$ אינו פרימיטיבי, אזי קיים יהא $\pi\in R$[3] אי פריק המחלק את כל מקדמי $f\cdot g$. נסמן:

$$f\left(x\right)=a_0+a_1x+...+a_nx^n,\ g\left(x\right)=b_0+b_1x+...+b_mx^m$$

יהא $k\leq n$ הגדול ביותר עבורו $\pi\nmid a_k$ ־ קיים כזה כי f פרימיטיבי[4]. באותה הצורה, יהא $j\leq m$ הגדול ביותר עבורו $\pi\nmid b_j$ ־ יש כזה כי g פרימיטיבי. אזי, π לא מחלק את המקדם של x^{k+j} בפולינום $f\cdot g$, שהרי:

$$f\cdot g=\sum_{i=1}^{n}a_ix^i\cdot\sum_{j=1}^{m}b_jx^j$$

המקדם של x^{k+j} אם כך יהיה:

$$...+a_{k-1}b_{j+1}+a_kb_j+a_{k+1}b_{j-1}+a_{k+2}b_{j-2}+...$$

נשים ♡ כי בסכום זה, כאמור π לא מחלק את a_kb_j ־ זאת כי הוא לא מחלק את a_k,b_j, ולכן בפרט גם את הכפל שלהם.

לכן הסכום הכולל לא יתחלק ב־π ־ כלומר, ה־gcd של המקדמים של הפולינום $f\cdot g$ לא יכול להיות π, בסתירה להנחה. ■

גם הכיוון השני של הטענה הזו נכונה ־ מושאר כתרגיל.

1.0.1 הלמה של גאוס

למה 1.27 יהא R תחום פריקות עם יחידה, ושדה שברים F, וכן $f\in R\left[x\right]$ פולינום. אם f ניתן להצגה כ־$f=g\cdot h$ עבור $g,h\in F\left[x\right]$, אזי קיימים $\overline{h},\overline{g}\in R\left[x\right]$ עבורם $f=\overline{g}\cdot\overline{h}$, כאשר:

$$\overline{g}=a\cdot g,\ \overline{h}=b\cdot h\ a,b\in F$$

[3] לא ה־gcd, אלא גורם שלו.

[4] כי אם π היה מחלק את כולם, אזי בפרט ה־gcd של המקדמים היה לפחות π ־ בסתירה לכך שהוא 1.

הוכחה: נניח $f = g \cdot h$. נמצא $a_1, a_2, b_1, b_2 \in F$, $\overline{g}, \overline{h} \in R[x]$ כך ש־$g = \frac{a_1}{a_2}\overline{g},\ h = \frac{b_1}{b_2}\overline{h}$, $\overline{g}, \overline{h} \in R[x]$ פרימיטיביים, a_1, a_2 זרים, b_1, b_2זרים בצורה הבאה:
$\frac{\alpha_1}{\alpha_2},\ \alpha_1, \alpha_2 \in R$. נכפול אותו בשבר, כאשר נגדיר את המונה $\hat{a}_1$ להיות ה־lcm של כל המכנים של המקדמים ואת המכנה $\hat{a}_2$ להיות ה־gcd של המקדמים שנקבל לאחר ההכפלה. הפולינום שיתקבל מהכפלה זו הוא ב־R, שכן כפלנו ב־lcm - כלומר הפכנו את כל המקדמים לשלמים, וחילקנו ב־gcd, ולכן לא קיבלנו לאחר מכן שברים. מכיון וחילקנו ב־gcd, הפולינום שהתקבל אכן פרימיטיבי. אם $\hat{a}_1, \hat{a}_2$ לא זרים נחלק אותם ב־gcd שלהם, ולאחר מכן נסמן $\hat{a}_1 = a_2, \hat{a}_2 = a_1$.
אזי, מהלמה הקודמת, $\overline{g} \cdot \overline{h}$ הוא גם פולינום פרימיטיבי. אזי:

$$f = g \cdot h = \frac{a_1}{a_2}\overline{g} \cdot \frac{b_1}{b_2}\overline{h} = \frac{a_1}{a_2} \cdot \frac{b_1}{b_2}\overline{g} \cdot \overline{h} = \frac{c_1}{c_2}\overline{g} \cdot \overline{h}$$

כאשר $\frac{a_1}{a_2} \cdot \frac{b_1}{b_2} = \frac{c_1}{c_2}$ לאחר צמצום, כלומר c_1, c_2 זרים.
קיבלנו כי f מתקבל מכפל של פולינום פרימיטיבי $\overline{g} \cdot \overline{h}$ ב־$\frac{c_1}{c_2}$, כאשר c_1, c_2 זרים. אבל מההגדרה, אין איבר בשדה המחלק את כל המקדמים של פולינום פרימיטיבי. לכן בהכרח c_2 הפיך, כלומר $\frac{c_1}{c_2} \in R$ - נסמנו ב־c, וקיבלנו כי $f = (c \cdot \overline{g}) \cdot \overline{h}$, כפי שרצינו. ■

ניסוח נוסף ללמה:

למה 1.28 אם R תחום פריקות, אזי גם $R[x]$ תחום פריקות (נובע מכך ש־$\mathbb{F}[x]$ תחום פריקות).

מסקנה 1.29 אם F שדה, אז מהלמה של גאוס $F[x]$ תחום פריקות. לכן:

$$F[x, y] \simeq (F[x])[y]$$

גם תחום פריקות. כך באינדוקציה נוכל להראות כי $F[x_1, x_2, ..., x_n]$ גם תחום פריקות.
ראינו מוקדם יותר כי אם R תחום נטרי בו כל אי פריק הוא ראשוני, אזי R תחום פריקות. הכיוון השני אינו נכון!
נשתמש בניתוח שעשינו מעלה - ראינו כי $F[x_1, x_2, ...]$ הינו תחום פריקות, אולם הוא לא נטרי! למשל, האידאל $(x_1, x_2, ...)$ לא נוצר סופית.

2 הרחבות של שדות

2.1 הגדרות

הגדרה 2.1 אם $F \subseteq E$ שדות, אזי E נקרא הרחבה של F אם $charF = charE$, וכן $F[x] \subseteq E[x]$.
במקרה זה נסמן E/F.

הגדרה 2.2 איבר $\alpha \in E$ נקרא אלגברי מעל F, אם יש $p \in F[x]$ כך ש־$p(\alpha) = 0$. אחרת, α נקרא טרנסצינדנטי (ביחס ל־F).

דוגמא: $F = \mathbb{Q},\ E = \mathbb{R}$, אזי $\sqrt{2}$ אלגברי מעל F, ו־e, π טרנסצינדנטיים.
עובדה פשוטה: כל $\alpha \in F$ הוא אלגברי מעל F.
דוגמא 2: יהא F שדה. נגדיר $E = F(t)$ ־ שדה הפונקציות הרציונליות במשתנה t = שדה השברים של חוג הפולינומים $F[t]$ ־ כלומר $F(t) = \left\{ \frac{p(t)}{q(t)} | p, q \in F[x] \right\}$.
אם האיבר $t \in E$ טרנסצינדנטי מעל F ־ נביט בהעתקה:

$$F[t] \to F(t)$$

כך ש־$x \to t$. העתקה זו היא חד חד ערכית ־ t עצמו הוא התמונה של העתקת הזהות.
דוגמא 3: $\mathbb{F}_P = \mathbb{Z}/(P)$, $p(x) = x^p - p$ ־ פולינום שונה מאפס, אבל $p(\alpha) = 0$ לכל $\alpha \in \mathbb{F}_P$.

הגדרה 2.3 אם E/F הרחבה, בפרט E מ"ו מעל F. מעלת ההרחבה היא המימד של E מעל F כמ"ו. נסמן:

$$|E : F| = |E/F| = dim_F E$$

דוגמאות:

- $|\mathbb{C} : \mathbb{R}| = 2$.
- $|\mathbb{R} : \mathbb{Q}| = \infty$.
- $|F(t) : F| = \infty$.

הגדרה 2.4 הרחבה נקראת סופית אם מעלת ההרחבה סופית, אחרת היא נקראת אינסופית.

28/2/2011

למה 2.5 יהא F שדה, ויהי $R \supseteq F$ תחום שלמות המכיל את F.
אם $dim_F R < \infty$ כמרחב וקטורי, אזי R שדה.

הוכחה: הדבר היחיד שיש לבדוק הוא קיום הופכי ־ כל שאר האקסיומות מתקיימות מההגדרה.
יהי $0 \neq r \in R$. הכפלה ב־r מהווה טרנספורמציה F לינארית של המרחב הוקטורי R ־ נסמן:

$$T_r : R \to R,\ a \to ra$$

העתקה זו מהגדרתה היא לינארית. מכיוון ו־R תחום שלמות, כלומר לא קיימים בו מחלקי אפס, לכן רק הכפלה של האיבר 0 ב־r תיתן 0 - כלומר, בהכרח הגרעין של T_r הוא טריוויאלי, ולכן, מכיוון ו־$dim_F R < \infty$, T_r הפיכה.

תזכורת - משפט קיילי המילטון: אם $T : V \to V$ ט"ל על מ"ו n מימדי (בפרט ממימד סופי), ו־$P_T = a_n x^n + ... + a_0$ הפולינום האופייני של T, אזי:

$$P_T(T) = 0$$

מסקנה: אם T הפיכה, אזי אם $a_0 \neq 0$, נקבל:

$$I = -\frac{a_n}{a_0}T^n - \frac{a_{n-1}}{a_0}T^{n-1} - ... - \frac{a_1}{a_0}T = T\left(-\frac{a_n}{a_0}T^{n-1} - ... - \frac{a_1}{a_2}I\right)$$

כאשר בסוגריים קיבלנו שוב פולינום ב־T - כלומר, T^{-1} הוא פולינום ב־T.
במקרה שלנו, נקבל כי קיים פולינום ב־r:

$$P_r = \alpha_{n-1}r^{n-1} + ... + \alpha_0,\ \alpha_i \in F\ \forall 1 \leq i < n$$

כך שהמכפלה ב־P_r הוא הטרנספורמציה ההפכית להכפלה ב־r - כלומר P_r הוא ההפכי ל־r, וכמובן ש־$P_r(r) \in R$ - כלומר, לכל $0 \neq r \in R$ קיים הפכי ב־R, כנדרש! ■

נביא הוכחה נוספת, פשוטה יותר: **הוכחה:** T_r חח"ע (כאמור כי R תחום שלמות), ומכיוון והיא מ־R לעצמו אזי T_r גם על, כלומר קיים $s \in R$ כך ש - $T_r(s) = 1$, כלומר $r \cdot s = 1$ - דהיינו $s = r^{-1}$, כנדרש! ■

הגדרה 2.6 יהיו $F \leq E$ הרחבת שדות, ויהי $\alpha \in E$. נסמן:

$$F[\alpha] = \{f(\alpha) \,|\, f \in F[x]\}$$

למה 2.7 עבור $\alpha \in E \geq F$, התנאים הבאים שקולים:

1. $dim_F F[\alpha] < \infty$.
2. α אלגברי.
3. $F[\alpha]$ הוא שדה.
4. $F[\alpha] = F(a)$.

לפני שנוכיח את הלמה הזו - נצטרך הגדרה ולמה נוספת:

הגדרה 2.8 $F(\alpha)$ הינו השדה המינימלי המכיל את F ואת α, כלומר:

1. $K = F(\alpha)$ $\bigcap_{E \supseteq K \supseteq F,\ \alpha \in K}$.
2. $F[x] = P, Q \Rightarrow F(\alpha) = \frac{P(\alpha)}{Q(\alpha)}$.

3. $F(\alpha)$ הוא שדה השברים של $F[\alpha]$.

תרגיל: הראה שקילות בין ההגדרות מעלה.

למה 2.9 אם $\alpha \in E \geq F$, אזי:

1. α אלגברי $\Leftrightarrow dim_F F[\alpha] < \infty$.
2. α טרנסצינדנטי $\Leftrightarrow F[\alpha] \simeq F[x]$.

נוכיח את הלמה מעלה, ובעזרתה נוכיח את הלמה 2.7. **הוכחה:** נוכיח את 1:
$\Leftarrow$ אם α אלגברי, אזי קיים $f \in F[x]$ כך ש־$f(\alpha) = 0$. נניח $deg(f) = n$. אזי $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ פורשים את $F[\alpha]$ כמרחב וקטורי. מדוע?
יהי $g \in F[x]$. אם $deg(g) < n$, ברור. אחרת נשתמש באלגוריתם אוקלידס ־ $F[x]$ הוא תחום אוקלידי ביחס לדרגת הפולינום ־ כלומר, ניתן לכתוב את פולינום זה כ־$g(x) = h(x) \cdot f(x) + r(x)$ עבור $h, r \in F[x]$ עבור $deg(r) < n$. אזי:

$$g(\alpha) = h(\alpha) \cdot f(\alpha) + r(\alpha) = h(\alpha) \cdot 0 + r(\alpha) = r(\alpha) \Rightarrow g(\alpha) = r(\alpha)$$

וכאמור $deg(r) < n$, לכן $g(\alpha) \in Span\left\{1, ..., \alpha^{n-1}\right\}$. זה נכון כאמור לכל $g \in F[x]$, ולכן $dim_F F[x] < \infty$.
נוכיח את 2:
אם α טרנסצינדנטי, אזי ההומומורפיזם הטבעי $F[x] \to F[\alpha]$ המוגדר ע"י $P(x) \to P(\alpha)$ הוא חח"ע[5], על כן זהו איזומורפיזם.
נשים ♡ כי בכיוון השני ל־1, $dim_F F[x] = \infty$, לכן אם $dimF[\alpha] < \infty$ אזי α אלגברי[6]. במקרה זה, גם הכיוון השני של 2 נגרר. ■

נוכיח את הלמה 2.7: **הוכחה:** מהלמה הקודמת $2 \Leftrightarrow 1$. בתחילת השיעור את הגרירה של 1 ל־3־ מהגדרתו, $F[\alpha]$ הוא חוג מעל השדה F, ומ־1 סופי, לכן הוא שדה מהלמה. ניתן להצדיק זאת גם על ידי משפט ממבנים 1 ־ תחום שלמות סופי הוא שדה.
3 גורר את 2 כי ראינו (בלמה הקודמת) שאם α טרנסצינדנטי, אז $F[\alpha] \simeq F[x]$, וזה לא שדה (כי אין הפכי ל־x), בסתירה.
$3 \Leftrightarrow 4$ נזכור כי שדה שברים הוגדר להיות השדה הקטן ביותר המכיל חוג כלשהוא. לכן, $F[\alpha]$ תמיד חלקי לשדה השברים שלו $F(\alpha)$ ־ אם $F[\alpha]$ שדה, נקבל שיוויון. אם הם שווים, אזי $F[\alpha]$ שווה לשדה השברים שלו, ולכן הוא שדה. ■

הגדרה 2.10 הרחבה $E \geq F$ תקרא אלגברית אם כל איברי E אלגבריים מעל F.

מסקנה 2.11 אם $F \leq E$ הרחבה סופית, אזי היא אלגברית.

הוכחה: לכל $\alpha \in E$, $F[\alpha] \in E$, ולכן $|E : F| > dim_F F[\alpha]$, ומכיוון וההרחבה סופית $|E : F| < \infty$, על כן $dim_F F[\alpha] < \infty$, ולכן, מהשקילות של 1 ו־2 בלמה 2.7, α אלגברי.■

למה 2.12 יהיו $F \leq E \leq L$ שדות. אזי:

$$|L : F| = |L : E| \cdot |E : F|$$

[5]אחרת היה פולינום f שאינו פולינום האפס אותו α מאפס, בסתירה לטרנסצינדנטיות.
[6]כי אז בהכרח קיים הגרעין לא טריוויאלי, לכן קיים פולינום ש־α מאפס שאינו טריוויאלי.

הוכחה: אם אחד מהשדות מדרגה ∞, אזי הטענה טריוויאלית.
אחרת, נניח $n = |E/F|$, $m = |L/E|$, וכן n, m סופיים. אזי, עלינו להוכיח כי $|L : F| = m \cdot n$.
יהיו $\alpha_1, ..., \alpha_n \in E$ המהווים בסיס ל־E מעל F, ויהיו $\beta_1, ..., \beta_m \in L$ המהווים בסיס ל־L מעל E. נראה כי $\{\alpha_i, \beta_j\}_{i,j=1}^{n,m}$ בסיס ל־L מעל F. תחילה, נראה כי הם **פורשים**:
יהי $b \in L$. אזי, מכיוון ו־$\beta_1, ..., \beta_m$ פורשים את L מעל E, יש $a_1, ..., a_m \in E$ כך ש:

$$b = \sum_{j=1}^{m} a_j \beta_j$$

באותה צורה, מכיוון ו־$\alpha_1, ..., \alpha_n$ פורשים את E מעל F, לכל $1 \leq j \leq m$ קיימים $c_{1_j}, ..., c_{n_j}$ כך ש:

$$a_j = \sum_{i=1}^{n} c_{i_j} \alpha_i$$

ויחדיו, נקבל:

$$b = \sum_{j=1}^{m} a_j \beta_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} c_{i_j} \alpha_i \right) \beta_j = \sum_{j=1}^{m} \sum_{i=1}^{n} c_{i_j} \alpha_i \beta_j$$

ולכן הם פורשים! נראה כי הם **בלתי תלויים לינארית**, ונסיים:
נניח כי $0 = \sum_{i,j=1}^{mn} c_{i_j} \alpha_i \beta_j$, ונראה כי לכל i, j - $c_{i_j} = 0$.
מכיוון ו־β_j בת"ל מעל E, אזי כל המקדמים שלהם שווים לאפס, כלומר לכל j, $0 = \left(\sum_{i=1}^{n} c_{i_j} \alpha_i\right)$. אבל, α_i בת"ל מעל F, ולכן $c_{i_j} = 0$ לכל i ולכל j - כנדרש! ■

"ללמה זו יש כמה מסקנות נחמדות"[7]:

משפט 2.13 תהי $F \leq E$ הרחבת שדות. אזי:

$$A = \{\alpha \in E | \alpha \text{ is an algebraic element over F}\}$$

הוא שדה!

הוכחה: אם α אלגברי מעל F, אזי מכיוון ש־$F\left(\alpha^{-1}\right) = F(\alpha)$, אזי $\left|F\left(\alpha^{-1}\right) : F\right| < \infty$.
לכן α^{-1} הוא אלגברי, כלומר A מכילה את ההפכי.
יהיו α, β אלגבריים. צריך להוכיח כי $\alpha \pm \beta,\ \alpha^{-1} \cdot \beta^{-1}$ גם אלגבריים - כלומר, הם גם ב־A. מהלמה, מספיק להראות כי $|F(\alpha, \beta) : F| < \infty$. אזי:

$$|F(\alpha, \beta) : F| = |F(\alpha, \beta) : F(\alpha)| \cdot |F(\alpha) : F| = |F(\alpha)(\beta) : F(\alpha)| \cdot |F(\alpha) : F|$$

השיוויון השני נובע מדיון קודם.
נביט בשני האיברים שקיבלנו - השמאלי הוא סופי מהלמה, כי β אלגברי מעל F, ולכן הוא אלגברי מעל $F(\alpha)$. האיבר הימני הוא גם סופי, שוב מהלמה - כי α אלגברי מעל F.
לכן בסה"כ הכפל של שני האיברים סופי, כנדרש! ■

[7] כן, צחיק מחבב את החומר הזה.

הגדרה 2.14 נסמן את הסגור האלגברי של F ב־E להיות:

$$\overline{F}^{E} = \{\alpha \in E | \alpha \text{ is an algebraic element over F}\}$$

מהמשפט שהוכחנו כרגע, זהו שדה.

הגדרה 2.15 נסמן את הסגור האלגברי של $\mathbb{Q}$ ב־$\mathbb{C}$ ב־$\overline{\mathbb{Q}} = \overline{\mathbb{Q}}^{\mathbb{C}}$. כאמור, זהו שדה, וכמו כן, עוצמתו בת מניה.

דוגמא: $\sqrt[3]{2} + \sqrt[5]{2} \in \overline{\mathbb{Q}}$, כמסקנה מהמשפט[8].
תרגיל:

1. יהי $\alpha \in \mathbb{C} \backslash \overline{\mathbb{Q}}$. אזי α טרנסצינדנטי מעל $\overline{\mathbb{Q}}$ (זהו מקרה פרטי של המסקנה הבאה).

2. הראו:

$$\left|\overline{\mathbb{Q}} : \mathbb{Q}\right| = \infty$$

מסקנה 2.16 תהי $E \geq F$ הרחבה אלגברית, $L \leq E$ הרחבה כלשהיא. אם $\alpha \in L$ אלגברי מעל E, אזי α אלגברי מעל F.

הוכחה: יהא $p(x) \in E[x]$ פולינום המאפס את α, כלומר $p(\alpha) = 0$. נסמן: $p(x) = \sum_{i=1}^{n} a_i x^i$, כאשר $a_i \in E$. לכל $0 \leq i \leq n$, a_i אלגברי מעל F כי E הרחבה אלגברית, ולכן, מהלמה 2.7, $|F(a_i) : F| < \infty$.
בנוסף, a_i אלגברי מעל $F(a_0, ..., a_{i-1})$. אזי, נקבל:

$$|F(a_0, ..., a_n) : F| = |F(a_0, ..., a_n) : F(a_0, ..., a_{n-1})| \cdot ... \cdot |F(a_0) : F| < \infty$$

הכפל קטן מ־∞ כי כל אחד מהאיברים הוא הרחבה אלגברית! לכן:

$$|F(\alpha) : F| \leq |F(\alpha, a_0, ..., a_n) : F| = |F(\alpha, a_0, ..., a_n) : F(a_0, ..., a_n)| \cdot |F(a_0, ..., a_n) : F|$$

הוכחנו כי האיבר הימני סופי, והאיבר השמאלי סופי שכן α מקיים פולינום שמתאפס ב־$F(a_0, ..., a_n)$. לכן הגודל סופי, וסיימנו! ■

טענה 2.17 תהי $F \leq E$ הרחבה כך ש־$E = F(\alpha)$ לאיזשהוא $\alpha \in E$ טרנסצינדנטי, ויהי $\beta \in F(\alpha) \backslash F$. אזי:

1. β טרנסצינדנטי מעל F.

2. α אלגברי מעל $F(\beta)$ - כלומר, $|F(\alpha) : F(\beta)| < \infty$.

[8] הסגור האלגברי הוא שדה, ולכן סגור לפעולת החיבור

הוכחה: נראה כי 2 מוביל ל־1, ולאחר מכן נראה כי 2 מתקיים ־ ונסיים.
אם $|F(\alpha):F(\beta)|<\infty$, אזי:

$$\underbrace{|F(\alpha):F|}_{=\infty \text{ because } \alpha \text{ is transcendental}} = \underbrace{|F(\alpha):F(\beta)|}_{<\infty}\cdot|F(\beta):F|$$

לכן $|F(\beta):F|=\infty$, כלומר β טרנסצינדנטי מעל F, וזה מראה כי 2 מוביל ל־1. נראה כי 2 מתקיים תמיד:
$\beta\in F(\alpha)$, לכן קיימים $Q,P\in F[x]$ כך ש־$\beta=\frac{P(\alpha)}{Q(\alpha)}$. נגדיר פולינום $f(x)\in(F(\beta))[x]$ כך ש־$f(x)=P(x)-\beta Q(x)$, אזי:

$$f(\alpha)=P(\alpha)-\beta Q(\alpha)=P(\alpha)-\frac{P(\alpha)}{Q(\alpha)}\cdot Q(\alpha)=P(\alpha)-P(\alpha)=0$$

כלומר מצאנו פולינום ש־α מאפס ב־$(F(\beta))[x]$, לכן α אלגברי מעל $F(\beta)$. ■

2.2 הרחבות אלגבריות פשוטות

1/3/2011

הגדרה 2.18 הרחבה $E\geq F$ נקראת פשוטה אם יש $\alpha\in E$ כך ש־$E=F(\alpha)$. אם α אלגברי, נסמן:

$$I_\alpha=\{f\in F[x]\,|\,f(\alpha)=0\}$$

אזי $I_\alpha\lhd F[x]$.

משפט 2.19 תהי $E\geq F$ הרחבה, ויהי $\alpha\in E$ אלגברי. אזי יש ב־I_α פולינום מתוקן אי פריק יחיד ־ נסמנו ב־m_α, והוא יקרא הפולינום המינימלי של α. מתקיים:

$$F[\alpha]\simeq {}^{F[x]}\!/_{I_\alpha},\ |F[\alpha]:F|=deg(m_\alpha)$$

הערה 2.20 ראינו בשיעור הקודם כי $F[\alpha]$ הוא שדה אם α אלגברי.

הוכחה: ברור כי I_α הוא אידאל, מהגדרתו. מכיוון ו־$F[x]$ הוא תחום ראשי, קיים $f\in I_\alpha$ יחיד עד כדי מכפלה בסקלר, כך ש־$I_\alpha=(f)$. נסמן את דרגתו ב־n.

טענה 2.21 f אי פריק.

הוכחה: אם בשלילה $f=g\cdot h$ עבור $g,h\in F[x]$ כך ש־g,h אינם סקלרים, אזי:

$$0=f(\alpha)=g(\alpha)\cdot h(\alpha)$$

לכן $g(\alpha)=0$ או $h(\alpha)=0$ ־ כלומר, אחד מהם ב־I_α. אבל, $deg(f)=deg(h)\cdot deg(g)$, ולכן $h,g\notin I_\alpha$ ־ שהרי f יוצר את I_α, כלומר כל האיברים בו הם כפולות של f, ובפרט מדרגה מינימלית n, בסתירה. ■

ראינו כבר כי ב־$F[x]$ חוג אוקלידי, f אי פריק $\Leftrightarrow$ $(f)=I_\alpha$ מקסימלי, ולכן $\Leftrightarrow$ ${}^{F[x]}\!/_{I_\alpha}$ שדה.

נביט בהעתקה $\psi : F[x] \to E$ המוגדרת ע"י $p(x) \to p(\alpha)$. זהו הומומורפיזם המקיים:

$$ker(\psi) = I_\alpha,\ Im(\psi) = F[\alpha]$$

ולכן, ממשפט הומומורפיזם של חוגים, $F[\alpha] \simeq {}^{F[x]}/_{I_\alpha}$.

עד כדי תיקון, $f = m_\alpha$. נניח $m_\alpha = x^n + a_{n-1}x^{n-1} + ... + a_0$ (אין מקדם a_n כי הפולינום המינימלי הוא מתוקן) הפולינום המינימלי של α. אזי $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ בת"ל מעל F, כי כל צירוף לינארי שלהם מתאים לפולינום ממעלה $deg(m_\alpha) = n >$ - וזה לא יתאפס ע"י α מהמינימליות של m_α. אבל אם $g \in F[x]$ פולינום כלשהוא, אזי אפשר למצוא (מהאוקלידיות) $h, r \in F[x]$ כך ש־$g = h \cdot m_\alpha + r$ כך ש־$deg(r) < n$ - לכן $g(\alpha) = r(\alpha)$ צירוף לינארי של $1, \alpha, \alpha^2, ..., \alpha^{n-1}$, ולכן $|F[\alpha] : F| = deg(m_\alpha)$. ■

מסקנה 2.22 תהי $F \leq E$ הרחבת שדות. אזי כל $\alpha \in E$ אלגברי מעל F. בפרט, לכל α אלגברי מעל F, כל $\beta \in F(\alpha)$ הוא אלגברי.

2.2.1 משפט Artin

משפט 2.23 תהא $E \geq F$ הרחבה סופית. אזי E פשוטה אמ"מ יש מספר סופי של שדות ביניים $F \leq K \leq E$.

לפני שנוכיח, נצטרך לפתח עוד כמה כלים:

למה 2.24 יהי $f \in F[x]$. אזי מספר השורשים של f ב־F $\leq deg(f)$.

הוכחה: נובע ישירות מכך שזהו תחום פריקות - שהרי שורשי f מתאימים לגורמים האי פריקים הלינאריים של f. ■

הגדרה 2.25 תהי G חבורה. $Exp(G) \in \mathbb{N} \cup \{\infty\}$ הוא ה־n המינימלי כך ש־$g^n = 1$ לכל $g \in G$. נשים ♡- תמיד $Exp(G) \leq |G|$.

למה 2.26 אם G אבלית סופית, אז יש איבר $g \in G$ עבורו $o(g) = Exp(G)$.

הוכחה: נסמן $Exp(G) = \prod_{i=1}^{k} p_i^{n_i}$. לכל $g \in G$, $o(g) = \prod_{i=1}^{k} p_i^{m_i(g)}$, כאשר $1 \leq m_i(g) \leq n_i$, זאת כי $o(g) | Exp(G)$, ובנוסף, לכל i, $n_i = \max_{g \in G}(m_i(g))$. לכן, לכל $1 \leq i \leq k$ קיים $g_i \in G$ כך ש־$m_i(g_i) = n_i$.

נגדיר את h_i להיות $h_i = g_i^{(\prod_{j \neq i} p_j^{m_j})}$. אזי, $o(h_i) = p_i^{n_i}$. לבסוף, נגדיר את g להיות $g = \prod_{i=1}^{k} h_i$. לכן נקבל:

$$o(g) = \prod_{i=1}^{k} p_i^{n_i} = Exp(G)$$

כנדרש! ■

מסקנה 2.27 חבורה סופית אבלית היא ציקלית אמ"מ $Exp(G) = |G|$.

טענה 2.28 יהא F שדה כלשהוא. אזי כל תת חבורה סופית של $F*$ היא ציקלית.

הוכחה: תהא $G \subseteq F*$ חבורה סופית (היא אבלית כי $F*$ אבלית). נניח $|G| = n$, $m = Exp(G)$.
כל $g \in G$ מקיים את המשוואה $x^m = 1$[9]. כמו לכל משוואה, מספר השורשים שלה $\geq$ מהמעלה, כלומר יש לכל היותר m איברים המקיימים את המשוואה הזו - לכן $n = |G| \leq m$. אי השיוויון ההפוך קיים מהגדרת $Exp(G)$, ולכן $Exp(G) = |G|$, כלומר, מהמסקנה של הלמה הקודמת, G ציקלית. ■

13/3/2011

עתה נוכיח את משפט ארטין:

משפט 2.29 תהא $E \geq F$ הרחבה סופית. אזי E פשוטה אמ"מ יש מספר סופי של שדות ביניים $F \leq K \leq E$.

הוכחה: $\Leftarrow$ נניח $E = F[\alpha]$ הרחבה סופית פשוטה - ראינו כי אם היא סופית, היא בפרט אלגברית. יהא $f \in F[x]$ פולינום מינימלי של α. אפשר להתייחס ל-f כפולינום ב-$E[x]$, שם הוא מתפרק בצורה יחידה למכפלה של גורמים אי פריקים (הרי ראינו שזה תחום פריקות) - נסמן פירוק זה ב- $f = f_1 \cdot ... \cdot f_r$.
יהיו $g_1, .., g_s$ כל המחלקים של f ב-$E[x]$ (הפריקים והאי פריקים), ונראה כי יש לכל היותר s שדות ביניים על ידי כך שנבנה התאמה חח"ע בין שדות הביניים לבין המחלקים - ואז מספר שדות הביניים יהיה סופי, שכן מספר המחלקים סופי.
יהיה K שדה ביניים, ויהיה $g \in K[x]$ פולינום מינימלי של α מעל K. אזי, g מחלק כל פולינום $h \in K[x]$ המקיים $h(\alpha) = 0$. בפרט $g|f$, לכן $g = g_i$ (עד כדי סקלר) לאיזה $1 \leq i \leq s$.
נותר להראות כי ההתאמה הזו היא חח"ע. נסמן $g(x) = \sum_{i=0}^{t} a_i x^i$, כאשר $a_i \in K$, וכן $a_t = 1$. נראה כי $K = F(a_0, ..., a_t)$, ולכן מ-g אפשר לשחזר את K באופן יחיד על ידי הגדרת המקדמים a_i, ולכן ההעתקה חח"ע. נסמן $L = F(a_0, ..., a_t)$. אזי $L \subseteq K$. g א"פ מעל K, והוא הפולינום המינימלי של α, וכן $E = K(\alpha)$, ולכן $|E : K| = deg(g)$. אבל g גם אי פריק מעל L, ולכן $|E : K| = |E : L|$, ולכן $K = L$.
$\Rightarrow$ אם $|F| < \infty$, ולכן גם $|E| < \infty$ - לכן $E*$ תת חבורה סופית, ולכן נוכל להשתמש בטענה הקודמת (שכן היא תת חבורה סופית של עצמה), כלומר קיים $\alpha \in E*$ כך ש- $E* = \langle \alpha \rangle$, ולכן $E = F(\alpha)$.
אחרת, $|F| = \infty$. נוכיח את הטענה באינדוקציה על $|E : F|$, שהוא מהנתון סופי.
בסיס האינדוקציה - עבור $|E : F| = 1$ הטענה ברורה, שכן אז $F = E$.
נסמן $n = |E : F| > 1$, ונניח כי הטענה מתקיימת עבור הרחבות מדרגה קטנה מ-n. נבחר $\beta \in E \backslash F$ כלשהוא. אזי $F[\beta] \supsetneq F$.

$$|E : F(\beta)| = \frac{|E : F|}{|F(\beta) : F|} < |E : F|$$

לכן מהנחת האינדוקציה, $E = (F(\beta))(\alpha)$ לאיזה $\alpha \in E$.
לכל $t \in F$, השדה $F(\beta + t\alpha)$ הוא שדה ביניים בין E ל-F. $|F| = \infty$ מהנחתנו, ויש רק קבוצה סופית של שדות ביניים, ולכן יש $t \neq s \in F$ כך ש-$F(\beta + t\alpha) = F(\beta + s\alpha)$. נסמן שדה זה ב-$K$. $\beta + t\alpha, \beta + s\alpha \in K$, ולכן $(t - s)\alpha \in K$, לכן גם $\alpha \in K$ ו-$\beta \in K$, ולכן $K = F(\alpha, \beta) = E$, כלומר $F(\beta + t\alpha) = E$. ■

[9] ישירות מהגדרת m.

מסקנה 2.30 כל הרחבה סופית של שדה סופי היא פשוטה.

הערה 2.31 אם $E \geq F$ הרחבה כך ש־$E = F(\alpha_1, ..., \alpha_n)$ עבור אילו $\alpha_1, ..., \alpha_n \in E$, נסמן $F \leq F(\alpha_1, ..., \alpha_n)$.

מסקנה 2.32 תהא $F \leq F(\alpha)$ הרחבה אלגברית פשוטה. אזי, כל שדה ביניים K הוא גם הרחבה פשוטה, כלומר $K = F(\beta)$ עבור איזשהוא $\beta \in K$.

2.3 הרחבות איזומורפיות

הגדרה 2.33 יהא $\varphi : F \to F'$ איזומורפיזם בין שדות.
φ מתרחב לאיזומורפיזם $\hat{\varphi} : F[x] \to F'[x]$, אם בהנתן $p(x) = \sum_{i=0}^{n} a_i x^i$, $\hat{\varphi}(p)(x) = \sum_{i=0}^{n} \varphi(a_i) x^i$.

הגדרה 2.34 הרחבות $F \leq E,\ F' \leq E'$ נקראות איזומורפיות, אם יש איזומורפיזם $\varphi : E \to E'$ כך ש־$\varphi(F) = F'$.

למה 2.35 יהי $\phi : F_1 \to F_2$ איזומורפיזם בין שדות, ויהיו $F_i \leq E_i$ הרחבות, כך ש־$\alpha_i \in E$ אלגברי מעל F_i עם פולינום מינימלי $p_i(x) \in F_i[x]$, ונניח $\hat{\phi}(p_1) = p_2$.
אזי, ϕ מתרחבת לאיזומורפיזם $\tilde{\phi} : F_1(\alpha_1) \to F_2(\alpha_2)$ המקיים $\tilde{\phi}(\alpha_1) = \alpha_2$.

הוכחה: ממשפט קודם, מכיוון ו־α_i אלגברי מעל F_i, $F_i(\alpha_i) \simeq {}^{F_i[x]}/_{(p_i)}$, והאיזומורפיזם ניתן על ידי $x + (p_i) \leftrightarrow \alpha_i$.
האיזומורפיזם $\phi : F_1 \to F_2$ מתרחב (מההגדרה) לאיזומורפיזם $\hat{\phi} : F_1[x] \to F_2[x]$ וכן $\hat{\phi}(p_1) = p_2$, לכן $\hat{\phi}((p_1)) = (p_2)$ (האידאלים הנוצרים על ידי הפולינום הללו), ועל כן העתקה זו משרה איזומורפיזם:

$$\tilde{\phi} : {}^{F_1[x]}/_{(\alpha_1)} \to {}^{F_2[x]}/_{(\alpha_2)}$$

הניתן על ידי:

$$\tilde{\phi}(q + (p_1)) = \hat{\phi}(q) + (p_2)$$

ובפרט:

$$\tilde{\phi}(x + (p_1)) = x + (p_2)$$

מכיוון ו־$F_i(\alpha_i) \simeq {}^{F[x]}/_{(p_i)}$, נקבל כי הרכבה של האיזומורפיזמים הנ"ל תיתן את האיזמורפיזם הנדרש. ■

מסקנה 2.36 תהא $F \leq E$ הרחבה, ויהא $p(x) \in F[x]$ פולינום אי פריק, ונניח $\alpha_1, \alpha_2 \in E$ שורשים שונים שלו. אזי, יש F־איזומורפיזם בין $F(\alpha_1)$ ל־$F(\alpha_2)$.

הוכחה: נציב בלמה הקודמת $F_1 = F_2 = F$, $E_i = F(\alpha_i)$. ■

דוגמא:
נביט ב־ $p(x) = x^4 - 2$ פולינום אי פריק מעל $\mathbb{Q}$ (מקריטריון אייזנשטיין), ויהא $\sqrt[4]{2} \in R_+$. אזי, $\mathbb{Q}[\sqrt[4]{2}] \simeq \mathbb{Q}[i\sqrt[4]{2}]$.

2.4 שדות פיצול

14/3/2011

הגדרה 2.37 יהי F שדה. נאמר שפולינום $f \in F[x]$ מתפצל (מעל F) אם קיימים איברים $a, \alpha_1, ..., \alpha_n \in F$ כך ש:

$$f(x) = a(x-\alpha_1) \cdot ... \cdot (x-\alpha_n)$$

אם E/F הרחבת שדה, $f \in F[x]$, ו־f מתפצל כפולינום ב־$E[x]$, אז נאמר ש־f מתפצל מעל E.

דוגמא:
$p(x) = x^4 - 1$ לא מתפצל מעל $\mathbb{Q}$, אבל כן מתפצל מעל $\mathbb{Q}[i]$, שם:

$$p(x) = (x+1)(x-1)(x+i)(x-i)$$

המשפט היסודי של האלגברה:

משפט 2.38 כל פולינום $p \in \mathbb{C}[x]$ מתפצל מעל $\mathbb{C}$.

הגדרה 2.39 יהי F שדה, $F \leq E$ הרחבה, ויהי $f \in F[x]$. E נקרא שדה פיצול של f אם f מתפצל מעל E, ואין שדה ביניים $F \subseteq K \subseteq E$ שבו הוא מתפצל.
הגדרה שקולה - אם f מתפצל מעל E, ו־E נוצר מעל F ע"י שורשי f ב־E.

למה 2.40 יהי $p(x) \in E[x]$, ונסמן $p(x) = a\prod_{i=0}^{n}(x-\alpha_i)$ כאשר $a, \alpha_i \in E$, אזי α_i הם השורשים היחידים של p הכל הרחבה $E \leq L$.

הוכחה: נניח $L \ni \alpha \neq \alpha_i$. אזי לכל i:

$$p(\alpha) = a\prod_{i=0}^{n}(\alpha - \alpha_i) \neq 0$$

■

למה 2.41 יהי F שדה, $f \in F[x]$ פולינום אי פריק. אזי יש הרחבה סופית $F \leq E$ בה ל־f יש שורש.

הוכחה: נגדיר $E = F[x]/(f)$. ראינו כי f אי פריק אמ"מ (f) מקסימלי, אמ"מ E שדה. אזי E מכיל עותק איזומורפי של F - נחשוב על E כעל הרחבה של F - הוא משוכן בו בתור סקלרים, החיתוך עם (f) הוא ריק, ולכן ההעתקה חח"ע.
אזי $|E:F| = deg(f) < \infty$. איברי E הם מהצורה $p(x) + (f)$ עבור $p \in F[x]$.
האיבר $x + (f)$ הוא שורש של הפולינום f, כי:

$$f(x + (f)) = f(x) + (f) = 0 + (f) = 0$$

כי $f(x) \in (f)$. ■

מסקנה 2.42 הלמה נכונה גם ללא ההנחה ש־f אי פריק.

הוכחה: יהא f_1 גורם אי פריק של f. נמצא הרחבה סופית $F \subseteq E$ בה ל־f_1 יש שורש. אזי, אותו שורש הוא גם שורש של f. ■

משפט 2.43 יהא F שדה, $p \in F[x]$. אזי קיימת הרחבה $F \leq E$ בה p מתפצל.

הוכחה: באינדוקציה על $deg(p)$.
בסיס - עבור $deg(p) = 1$ הטענה ברורה (שדה הפיצול הוא השדה המקורי).
נניח כי $n = deg > 1$, וכי המשפט נכון עבור פולינומים ממעלה $< n$ מעל כל שדה.
מהלמה ומהמסקנה, ישנה הרחבה סופית $E' \geq F$ בה ל־p יש שורש, $\alpha_0 \in E'$ - נרשום $p(x) = (x - \alpha_0) \cdot g(x)$ עבור $g \in E'[x]$, כאשר $deg(g) = n - 1$. אזי, נוכל להשתמש בהנחת האינדוקציה - כלומר, קיימת הרחבה סופית $E \geq E'$ בה g מתפצל, כלומר:

$$g(x) = a\prod_{i=1}^{n}(x - \alpha_i),\ \alpha_i \in E$$

לכן $p(x) = a\prod_{i=0}^{n}(x - \alpha_i)$, כאשר $|E : F| = |E : E'| \cdot |E' : F| < \infty$. ■

דוגמא:
$p(x) = x^2 + 1,\ F = \mathbb{R}$. שדה הפיצול שלו הוא $E = \mathbb{R}[x]/(x^2+1)$.
האיבר $\alpha = x + \left(x^2 + 1\right)$ מקיים $\alpha^2 = -1$, כי:

$$\alpha^2 + 1 = x^2 + \left(x^2 + 1\right) + 1 = 0 + \left(x^2 + 1\right)$$

כלומר הוא שורש של $p(x)$. כמו כן, $\mathbb{R}[x]/(x^2+1)$ עם $\alpha \to i$.

למה 2.44 אם $f \in F[x]$ מתפצל ב־E עבור הרחבה $F \leq E$, אזי יש שדה פיצול יחיד ל־f המוכל ב־E (ומכיל את F).

הוכחה: נרשום $f(x) = a\prod_{i=1}^{n}(x - \alpha_i)$ $a \in F$ $\alpha_i \in E$ מוגדרים היטב (כלומר, הם השורשים היחידים של f). לכן כל שדה ביניים $F \leq K \leq E$ בו f מתפצל, חייב להכיל גם $\alpha_1, .., \alpha_n$. לכן קיים שדה מינימלי בו הפולינום מתפצל, והוא $F(\alpha_1, .., \alpha_n)$. ■

מסקנה 2.45 לכל שדה F ולכל פולינום $p \in F[x]$ יש שדה פיצול $F \leq E$.

הערה 2.46 שדה פיצול של פולינום הוא תמיד הרחבה סופית.

משפט 2.47 יהא $\phi : F_1 \to F_2$ איזומורפיזם של שדות, ויהיו $p_i \in F_i[x]$ פולינומים כך ש־$p_2 = \hat{\phi}(p_1)$, ויהא $F_i \leq E_i$ שדה פיצול של p_i. אזי ϕ מתרחב לאיזומורפיזם מ־E_1 ל־E_2.

הוכחה: באינדוקציה על $n = deg(p_i)$.
בסיס - עבור $n = 1$ הטענה ברורה, כי $E_i = F_i$.

נניח כי הטענה נכונה עבור פולינומים מדרגה n. נסמן: $p_1 = f_1^1 \cdot f_1^2 \cdot ... \cdot f_1^k$ מכפלה של אי פריקים כך ש־$f_1^i \in F_1[x]$. אזי מהנתון $p_2 = \hat{\phi}(p_1) = \hat{\phi}(f_1^1) \cdot ... \cdot \hat{\phi}(f_1^k)$. נסמן $p_2 = f_2^1 \cdot ... \cdot f_2^k$. אזי $\hat{\phi}(f_1^i) = f_2^i$.
נבחר $\alpha \in E_1$ שורש של f_1^1 וכן $\beta \in E_2$ שורש של f_2^1. ראינו כי האיזומורפיזם $\phi : F_1 \to F_2$ מתרחב לאיזומורפיזם $\overline{\phi} : F_1[\alpha] \to F_2[\beta]$ המקיים $\overline{\phi}(\alpha) = \beta$. נסמן $E_1' = F_1[x],\ E_2' = F_2[x]$ - אזי $\overline{\phi} : E_1' \to E_2'$ מרחיב את ϕ. נסמן:

$$p_1 = (x-\alpha) \cdot g_1,\ p_2 = (x-\beta) \cdot g_2$$

מכיוון ו־$p_2 = \overline{\phi}(p_1) = \hat{\phi}(\overline{\phi}(p_1))$, נקבל כי:

$$\hat{\phi}(\overline{\phi}((x-\alpha)g_1)) = \hat{\phi}(\overline{\phi}(x-\alpha))\,\hat{\phi}(\overline{\phi}(g_1)) = (x-\beta)g_2$$

ולכן $g_2 = \hat{\phi}(\overline{\phi}(g_1))$. בנוסף, $F_i \leq E_i$ שדה הפיצול של g_i, וכן $deg(g_i) = n-1$, ולכן מהנחת האינדוקציה האיזומורפיזם מתרחב. ■

מסקנה 2.48 יהי $f \in F[x]$, ויהיו E_1, E_2 שדות פיצול של f מעל F. אזי קיים $\varphi : E_1 \to E_2$ איזומורפיזם מעל F.

2.5 שדות סגורים אלגברית וסגור אלגברי

הגדרה 2.49 שדה E נקרא סגור אלגברית אם כל פולינום ב־$E[x]$ מתפצל.

הגדרה 2.50 יהי F שדה. שדה E נקרא סגור אלגברי של F אם E/F הרחבה אלגברית, וכל פולינום ב־$F[x]$ מתפצל מעל E.

אבחנה: נניח E/F הרחבה אלגברית, ו־K/E. אזי K הוא סגור אלגברי של E אמ"מ הוא סגור אלגברי של F. מיד נראה מדוע זה נכון.

טענה 2.51 תהי E/F הרחבה אלגברית. אזי התנאים הבאים שקולים:

1. E סגור אלגברית.
2. E הסגור האלגברי של F.
3. אם L/F הרחבה אלגברית, ו־$L \supseteq E$, אז $L = E$.
4. אם L/E הרחבה אלגברית, אז $L = E$.

הוכחה: $1 \Leftarrow 2$: נובע ישירות מההגדרה.
$2 \Leftarrow 3$: יהי $\alpha \in L$. לפי ההנחה, L/F הרחבה אלגברית, ולכן α אלגברי מעל F. יהי $g \in F[x]$ הפולינום המינימלי של α מעל F. g מתפצל מעל E (כי E הוא הסגור האלגברי של F). כלומר, קיימים $b, \beta_1, ..., \beta_r \in E$ כך ש־$g(x) = b(x-\beta_1) \cdot ... \cdot (x-\beta_r)$. $g(\alpha) = 0$, לכן $\alpha = \beta_i$ עבור איזשהוא i, לכן $\alpha \in E$. זה נכון לכל α כאמור, לכן ההכלה בכיוון שאינו נתון מתקיימת, ומהכלה דו כיוונית נקבל כי $L = E$.
$3 \Leftarrow 4$ הרחבה אלגברית של הרחבה אלגברית היא אלגברית, ולכן אם L/E אלגברית, גם L/F אלגברית, ואז מהתנאי השלישי נקבל את השיוויון הדרוש.

$4 \Leftarrow 1$ יהי $f \in F[x]$. קיים שדה פיצול L/E של f (זוהי הרחבה אלגברית). לפי ההנחה $L = E$, כלומר f מתפצל מעל E. ■

כעת נוכיח את האבחנה: **הוכחה:** K/E הרחבה אלגברית $\Leftrightarrow$ K/F אלגברית, ולפי הטענה K סגור אלגברי של $F \Leftrightarrow K$ סגור אלגברית $\Leftrightarrow K$ הוא סגור אלגברי מעל F. ■

טענה 2.52 נניח K שדה סגור אלגברית, ו־$F \subseteq K$ שדה, ונסמן:

$$E = \{x \in K | \text{x is an algbraic element over F}\}$$

אזי, E הוא הסגור האלגברי היחיד של F בתוך K.

דוגמא: אנו מאמינים ש־$\mathbb{C}$ סגור אלגברית. לכן, שדה המספרים האלגבריים מעל $\mathbb{Q}$ בתוך $\mathbb{C}$ הוא סגור אלגברי של $\mathbb{Q}$. נסמנו (כפי שראינו בעבר) ב־$\overline{\mathbb{Q}}$.

נוכיח את הטענה: **הוכחה:** נראה כי E סגור אלגברית. נניח ש־$0 \neq f \in E[x]$ פולינום אי פריק כך ש־$deg(f) \geq 1$. נראה ש־$deg(f) \leq 1$ (ולכן שווה ל־1).

K סגור אלגברית, ולכן f מתפצל מעל K. יהי $\alpha \in K$ שורש של f. α אלגברי מעל E (כי f לדוגמא מאפס אותו), E/F הרחבה אלגברית, ולכן α אלגברי מעל F.

מכאן $\alpha \in E$, לכן $(x-\alpha) | f$, ומכיון ו־f אי פריק מהנחתנו, $f(x) = b(x-\alpha)$, כלומר E סגור אלגברית (כי כל פולינום א"פ הוא מדרגה 1, כלומר כל הפולינומים מתפצלים), ולכן, מהטענה הקודמת, E הוא הסגור האלגברי של F.

נותר להראות כי E סגור אלגברי יחיד ב־K. נניח $F \subseteq L \subseteq K$ סגור אלגברי של F.

ראשית נראה כי $L \supseteq E$: יהי $\alpha \in E$. α אלגברי מעל F (מהגדרת E). יהי g הפולינום המינימלי של α מעל F. g מתפצל מעל L, לכן שורשיו ב־L הם כל שורשיו ב־K. מכיוון ו־$g(\alpha) = 0$, הרי ש־α שורש של g, ולכן $\alpha \in L$.

מצד שני, L/F הרחבה אלגברית, ולכן L/E אלגברית. מכיוון ו־E סגור אלגברית, אזי מהטענה, נקבל ישירות כי $L = E$, כנדרש. ■

2.5.1 קיום הסגור האלגברי

משפט 2.53 לכל שדה יש סגור אלגברי.

נזכר ב**למה של צורן** מהקורס תורת הקבוצות:

למה 2.54 תהי $(E, \leq)$ קבוצה סדורה חלקית לא ריקה, ונניח שלכל שרשרת ב־S יש חסם מלעיל. אזי יש ב־S איבר מקסימלי.

בעזרת הלמה הנ"ל (שלא נוכיח), נוכיח את קיום הסגור האלגברי. כך לפני כן ־ טענת עזר:

טענה 2.55 תהי E/F הרחבה אלגברית. אזי $|E| = \aleph_0 \cdot |F|$.

הוכחה: לאיבר $\alpha \in E$ נתאים זוג סדור (m_α, α), כאשר m_α הוא הפולינום המינימלי של α מעל F. זו העתקה חח"ע מ־E ל־$F[x] \times E$. לכל $g \in F[x]$ יש לכל היותר מספר סופי של איברים α כך ש־(g, α) נמצא בתמונת ההעתקה הזו (כי α צריך להיות שורש של g), ולכן:

$$|E| \leq |F[x]| \cdot \aleph_0 = |F| \cdot \aleph_0 \cdot \aleph_0 = |F| \cdot \aleph_0$$

■

כעת, להוכחת המשפט: **הוכחה:** יהי F שדה. ניקח קבוצה Ω שעוצמתה $2^{|F|}\cdot\aleph$. נתבונן בזוגות (E,ξ) כאשר $E\subseteq\Omega$, ו־ξ מבנה של שדה על E - $(\cdot,+,1,0)$. נקבע אחת ולתמיד זיהוי של F עם קבוצה המוכלת ב־Ω, שנסמנה ב־F. ב־$\mathcal{F}$ נסמן את מבנה השדה של F, כלומר $(F,\mathcal{F})$ הוא השדה איתו התחלנו.

על קבוצת כל הזוגות הללו נגדיר יחס סדר חלקי:

$(E_1,\xi_1)\leq(E_2,\xi_2)\Leftrightarrow E_1\subseteq E_2$, וגם המבנה ξ_2 מצומצם ל־E_1 שווה ל־ξ_1.

נצטמצם לקבוצת הזוגות:

$$S=\{(E,\xi)\,|\,(F,\mathcal{F})\leq(E,\xi)\}$$

כלומר קבוצת הזוגות המהווים הרחבה אלגברית ל־$(F,\mathcal{F})$. זוהי אינה קבוצה ריקה, כי $(F,\mathcal{F})$ שייכת לה.

נניח $\{(E_\alpha,\xi_\alpha)\}$ שרשרת ב־S. נביט ב־$E=\cup E_\alpha$. לכל $x,y\in E$ קיים α כך ש־$x,y\in E_\alpha$, ונגדיר את החיבור והכפל של שני איברים אלו כאיבר המתאים ב־E_α. הגדרה זו אינה תלויה ב־α מאחר ומבנה השדות תואם תמיד - כלומר, זהו חסם מלעיל של השרשרת.

לכן, לפי הלמה של צורן, יש ב־S איבר מקסימלי - נסמנו ב־$(K,\mathcal{K})$.

נזכור כי E/F הרחבה אלגברית, כי כל איבר בו אלגברי מעל F.

K/F הרחבה אלגברית, כי $(K,\mathcal{K})$ ב־S. נניח בשלילה כי K איננו הסגור האלגברי של F. אזי, קיימת הרחבה אלגברית L/K כך ש־$K\subsetneq L$ (מהטענה הקודמת).

L הרחבה אלגברית של F, ולכן מהלמה $|L|\leq\aleph_0\cdot|F|$, וכן: $|\Omega\backslash K|\geq\aleph_0\cdot|F|$, לכן ניתן לשכן את L ב־Ω (כקבוצה), כך שנקבל זוג $(L,\mathcal{L})$ השייך ל־S ומכיל את $(K,\mathcal{K})$. מהיות איבר זה המקסימלי ב־S נקבל כי $K=L$, בסתירה להנחה. ■

15/3/2011

הערה 2.56 בהוכחה למעלה יש טעות[10] -

$$|F[x]|=\begin{cases}\aleph_0 & |F|<\infty\\ |F| & otherwise\end{cases}$$

לכן בהוכחת המשפט יש להשתמש ב־$|\Omega|\geq 2^{|\aleph_0|\cdot F[x]}$.

משפט 2.57 תהי E_1/F_1 הרחבה אלגברית, ויהי E_2/F_2 סגור אלגברי, וכן יהי $\varphi:F_1\to F_2$ איזומורפיזם.

אזי, קיימת הרחבה $\psi:E_1\to E_2$ מונומורפיזם (לתוך E_1) של φ. יתרה מזו, אם E_1 סגור אלגברית, אזי ψ הוא איזומורפיזם.

הוכחה: נגדיר $S=\left\{(L,\psi)\,|F_1\subseteq L\subseteq E_1,\ \psi:L\overset{mono}{\to}E_2,\ \psi|_{F_1}=\phi\right\}$, ונגדיר סדר חלק על איברי S באופן הבא:

$(L_1,\psi_1)\leq(L_2,\psi_2)$ אמ"מ $L_1\subseteq L_2$, $\psi_2|_{L_1}=\psi_1$.

נראה שמתקיימים תנאי הלמה של צורן:

ראשי, S אינה ריקה, כי $(F_1,\varphi)\in S$.

שני,ת, אם (L_α,ψ_α) שרשרת ב־S, אזי $(\cup L_\alpha,\cup\psi_\alpha)$ שייך ל־S, והוא חסם מלעיל ($\cup\psi_\alpha$ מוגדר היטב כפונקציה בכלל תנאי ההתאמה בתוך השרשרת).

על כן, לפי הלמה של צורך, יש ב־S איבר מקסימלי - נסמנו ס־(L,ψ). הטענה הראשונה תוכח אם נראה כי $L=E_1$.

[10] זניחה לדעת שפחתכם הנאמנה.

נניח בשלילה כי $L \neq E_1$. יהי $\alpha \in E_1 \backslash L$. α אלגברי מעל F_1, ולכן גם מעל L. יהי $g \in L[x]$ הפולינום המינימלי של α מעל L. אזי $L[\alpha] \simeq {}^{L[x]}/_{(g)}$. מצד שני, g אי פריק מעל L, ולכן $\tilde{\psi}(g)$ אי פריק מעל מעל $\psi(L)$. מכיוון ש־E_2 סגור אלגברית, יש ל־$\tilde{\psi}(g)$ שורש ב־E_2 ־ נסמנו ב־β.

יש איזומורפיזם $\psi(L)[\beta] \simeq {}^{\psi(L)}/_{(\tilde{\psi}(g))}$ מעל $\psi(L)$. לפיכך, ניתן להרחיב את ψ לאיזומורפיזם $\rho : L[\alpha] \to \psi(L)[\beta]$, בסתירה למינימליות. לפיכך $(L, \psi) = (E_1, \psi)$.

נניח כי E_1 הוא סגור אלגברי של F_1. אז E_1 סגור אלגברית, ולכן $\psi(E_1)$ סגור אלגברית. ואז, E_2 הרחבה אלגברית של $\psi(E_1)$. על פי טענה מההרצאה הקודמת, נובע כי $\psi(E_1) = E_2$. ■

מסקנה 2.58 כל שני סגורים אלגבריים של שדה F הם איזומורפיים.

סימון: (כבר ראינו בעבר) ־ אם F שדה, מסמנים את הסגור האלגברי שלו ב־$\overline{F}$.

הערה 2.59 אין יחידות של איזומורפיזם בין סגורים אלגבריים.

דוגמא: יודעים שקיים איזומורפיזם:

$$\varphi : \mathbb{Q}\left[\sqrt{2}\right] \to \mathbb{Q}\left[-\sqrt{2}\right], \ \sqrt{2} \to -\sqrt{2}$$

מהמשפט נובע שקיים איזומורפיזם $\psi : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ המקיים $\psi\left(\sqrt{2}\right) = -\sqrt{2}$.
שאלה: האם נוכל להגדיר ψ כזה מ־$\mathbb{R}$ ל־$\mathbb{R}$?

2.5.2 המשפט היסודי של האלגברה

משפט 2.60 יהי $p \in \mathbb{C}[x]$ פולינום לא קבוע. אזי קיים ל־p שורש ב־$\mathbb{C}$.

תזכורת: אינדקס של מסילה סגורה הוא:

$$\gamma : [0,1] \to \mathbb{R}^2 / \{(0,0)\}$$

"מספר הפעמים שהמסילה הקיפה את הראשית", ונסמן $i(\gamma)$.

משפט 2.61 אם γ_1, γ_2 מסילות הומוטיפיות ב־$\mathbb{R}^2 / \{(0,0)\}$, אזי $i(\gamma_1) = i(\gamma_2)$.

לא נוכיח משפט זה, אך נשתמש בו על מנת להוכיח את המשפט היסודי של האלגברה:
הוכחה: נניח בשלילה של־p אין שורש ב־$\mathbb{C}$. אזי נתבונן במסילות מהצורה:
....
בהמשך! ■

3 תורת גלואה

תהא $F \leq E$ הרחבת שדות סופית.

הגדרה 3.1 $Gal\left(E/F\right)$ היא חבורת ה־F־אוטומורפיזמים של E.
כלומר, איברי $Gal\left(E/F\right)$ הם אוטומורפיזמים של השדה E המקבעים את איברי F.
דהיינו, $\sigma \in Gal\left(E/F\right)$ היא העתקה חח"ע ועל מ־E לעצמו, המקיימת:

$$\forall a,b \in E \sigma\left(a \cdot b\right) = \sigma\left(a\right) \cdot \sigma\left(b\right) \tag{1}$$
$$\sigma\left(a+b\right) = \sigma\left(a\right) + \sigma\left(b\right) \tag{2}$$
$$\forall f \in F \sigma\left(f\right) = f \tag{3}$$

לדוגמא:

$$\mathbb{Z}/(2) \simeq Gal\left(\mathbb{C}/\mathbb{R}\right)$$

נזכור כי $(-i)^2 = -1,\ i^2 = -1$.
אזי, כל $\sigma \in Gal\left(\mathbb{C}/\mathbb{R}\right)$ מקיים $\sigma\left(i\right) = \pm i$.
אם $\sigma\left(i\right) = i$, אז σ היא העתקת הזהות, אחרת אם $\sigma\left(i\right) = -i$, אזי σ היא הצמדה.

נסמן את $\mathcal{F} = \{F \leq K \leq E\}$ להיות קב' כל שדות הביניים, וכן $G = Gal\left(E/F\right)$.
תחת סימון זה, נסמן ב־ $\mathcal{G} = \{H \leq G\}$ את קב' כל תתי החבורות. נראה בהמשך כי $\mathcal{G}$ היא סופית תמיד.

הגדרה 3.2 עבור תת חבורה $H \leq G$, נגדיר את קבוצת נק' השבת בצורה הבאה:

$$Fix\left(H\right) = \{a \in E | h\left(a\right) = a\ \forall h \in H\}$$

נשים ♡ כי תמיד $Fix\left(H\right)$ מכיל את F, ישירות מההגדרה.

נסמן שתי העתקות:

$$f : \mathcal{G} \to \mathcal{F}\ H \to Fix\left(H\right),\ g : \mathcal{F} \to \mathcal{G}\ K \to Gal\left(E/K\right)$$

כאשר $Gal\left(E/K\right)$ היא כאמור קבוצת האוטומורפיזמים המקבעים את K, ובפרט מוכלים ב־$Gal\left(E/F\right)$.
אופטימלית, g, f הופכיות זו לזו, אבל זה לא תמיד נכון! זה נכון במקרה מסויים אותו נראה בהמשך.
אם זאת, נחקור אילו תכונות תמיד יתקיימו:

למה 3.3 f, g מקיימות את התכונות הבאות:

$$\forall H \leq Gg\left(f\left(H\right)\right) \supseteq H,\ \forall F \leq K \leq E\ f\left(g\left(K\right)\right) \supseteq K \tag{4}$$
$$\forall H_1, H_2 \subseteq GH_1 \subseteq H_2 \Rightarrow f\left(H_1\right) \supseteq f\left(H_2\right) \tag{5}$$
$$F \leq K_1 \leq K_2 \leq E \Rightarrow g\left(K_1\right) \supseteq g\left(K_2\right) \tag{6}$$

הגדרה 3.4 באופן כללי, במצב בו הפונקציות f,g בין שתי קבוצות מקיימות את התנאים מעלה, מצב זה נקרא בשם התאמת גלואה.

הוכחה: 1: תהי $G \geq H$ תת חבורה. $f(H) = K$ הוא שדה כל האיברים ב־E המקובעים על ידי כל איברי H. כמו כן, $g(f(H)) = g(K)$ הוא חבורת כל אברי G המקבעים את K. לכן $g(K)$ מכיל לפחות את H. החלק השני מוכח באופן אנלוגי.
2: יהיו $H_1 \leq H_2$ תתי חבורות של G. אזי:

$$f(H_1) = \{a \in E | h(a) = a \ \forall h \in H_1\}$$

לחבורה גדולה מ־H_1 המכילה אותה יהיה אותו מספר של נקודות שבת או פחות 0 ובוודאי שלא יותר, ולכן:

$$f(H_1) \supseteq \{a \in E | h(a) = a \ \forall h \in H_2\} = f(H_2)$$

3 מוכח בצורה דומה. ■

למה 3.5 נגדיר:

$$\mathcal{F}_0 = \{f(H) | H \leq G\}, \ \mathcal{G}_0 = (g(K))\{g(K) | F \leq K \leq E\}$$

אזי $g : \mathcal{F}_0 \to \mathcal{G}_0$, $f : \mathcal{G}_0 \to \mathcal{F}_0$ חח"ע ועל והופכיות זו לזו, ומתקיים:

$$\mathcal{F}_0 = \{F \leq K \leq E | K = f(g(K))\} \tag{7}$$
$$\mathcal{G}_0 = \{H \leq G | H = g(f(H))\} \tag{8}$$

הוכחה: נוכיח את התנאים 1 ו־2, ושאר הטענה תנבא ישירות.
נראה הכלה דו כיוונית: לתנאי הראשון:
יהא $F \leq K \leq E$ המקיים $K = f(g(K))$[11] ברור כי $K \in \mathcal{F}_0$, מההגדרה.
בכיוון השני, נניח כי $K \in \mathcal{F}_0$, כלומר $K = f(H)$ לאיזה תת חבורה $H \leq G$. עלינו להראות כי $K = f(g(K))$. מהתנאי הראשון בלמה הקודמת, אנו יודעים כי $K \subseteq f(g(K))$. כמו כן, מאותו התנאי בלמה הקודמת: $H \supseteq g(f(H)) = g(K)$. לכן, מהתנאי השני בלמה זו, נקבל:

$$f(g(K)) \subseteq f(H) = K$$

לכן מהכלה דו כיוונית התנאי הראשון נכון. החלק השני נותר כתרגיל - אולם מוכח באופן דומה. ■

28/3/2011

הגדרה 3.6 הרחבה סופית $E \geq F$ נקראת הרחבת גלואה, אם:

$$Fix(Gal(E/F)) = F$$

[11] מכיוון והסימון $\leq$, בטוח כי F ו־E מקיימים את התנאי - ועל כן קיים כזה.

למה 3.7 תהא E/F הרחבת שדות סופית, ותהי $G = Gal(E/F)$, וכן $p \in F[x]$, ונסמן את קבוצת כל השורשים של p ב־Ω. אזי:

1. G פועלת בתמורות על Ω.
2. אם $E = F(\Omega)$, G איזומורפית לתת חבורה של $sym(\Omega)$.
3. אם p אי פריק ו־E שדה פיצול של $q \in F[x]$, אז G פועלת טרנזיטיבית על Ω.

הוכחה: 1 - מהגדרת פעולה, עלינו להראות כי כל איבר ב־G ניתן לפרש כפונקציה מהקבוצה לעצמה - במקרה שלנו, ל־$S = sym(\Omega)$. על כן, מספיק להראות כי הפעולה של G על Ω היא תמורה.
אם $\alpha \in \Omega, \sigma \in G$, אזי:

$$p(\alpha) = 0 \Rightarrow \sigma(p(\alpha)) = \sigma(0) = 0 \Rightarrow p(\sigma(\alpha)) = \sigma(p(\alpha)) \Rightarrow \sigma(\alpha) \in \Omega$$

כאשר המעבר השני משמאל נכון כי מקדמי p ב־F, ו־σ כאמור משמרת את F.
על כן $\sigma(\Omega) \in \Omega$, אבל σ חח"ע וכמו כן Ω סופית, ולכן σ חח"ע ועל Ω, כלומר היא תמורה - ולכן התנאי הראשון מתקיים.
2 - נניח כעת כי $E = F(\Omega)$.
עובדה כללית: אם G פועלת על קבוצה X, וכן $Y \subseteq X$ תת קבוצה G־אינווריאנטית, כלומר כל איבר ב־G מקבע אותה, אזי העתקת הצמצום מ־G ל־$Sym(Y)$ היא הומומורפיזם.
מהעובדה מעלה, ההעתקה $G \xrightarrow{r} Sym(\Omega)$ המצמצמת כל איזומורפיזם לקבוצת שורשי p ב־E היא הומומורפיזם. על כן, נותר להוכיח כי r חח"ע. נראה כי הגרעין שלו הוא טריוויאלי:
נניח כי $\sigma \in ker(r)$. כלומר לכל $\alpha \in \Omega$, $\sigma(\alpha) = \alpha$. אזי $Fix(\sigma)$ הוא שדה המכיל את F ואת Ω - כי הוא מכיל את כל האיברים ב־E המקובעים על ידי σ - היא ב־$Gal(E/F)$ ולכן מקבעת את כל F, וכן אנו מניחים כי היא מקבעת גם את כל Ω מהגדרתה. לכן $E = F(\Omega) \subseteq Fix(\sigma)$, כלומר $\sigma = id$. לכן r חח"ע, כלומר G איזומורפית לתת חבורה $Sym(Y) \subseteq r(G)$.
3 - נניח כי p אי פריק, וכן E שדה פיצול של $q \in F[x]$. יהיו $\alpha, \beta \in \Omega$ שורשים של p. מכיוון ו־p אי פריק, ישנו F־איזומורפיזם $F(\alpha) \xrightarrow{\sim} F(\beta)$ $f : F(\alpha) \xrightarrow{\sim} F(\beta)$. E שדה פיצול של q מעל F, לכן מעל $F(\beta), F(\alpha)$, ממשפט שראינו, f מתרחב לאיזומורפיזם $\tilde{f} : E \to E$, לכן $\tilde{f} \in G$, ומתקיים: $\tilde{f}(\alpha) = \beta$. ■

מסקנה 3.8 בהנחות של תנאי 3, אם ל־p שורש ב־E, אזי הוא מתפצל מעל E.

הוכחה: יהא $F \subseteq E \subseteq \overline{F}$ סגור אלגברי של F, ויהא $\alpha \in E$ שורש של p, ויהא $\beta \in \overline{F}$ שורש כלשהוא של p. עלינו להראות כי $\beta \in E$.
p אי פריק, לכן קיים F־איזומורפיזם $f : F(\alpha) \xrightarrow{\sim} F(\beta)$.
יהא $\tilde{E}$ שדה הפיצול של q מעל $F(\beta)$. אם Λ - קבוצת שורשי q ב־E, אזי $E = F(\Lambda)$ (כי E הוא כאמור שדה הפיצול של q) . מקדמי q הם ב־F ולכן $\overline{f}(g) = g$ (פונקציית ההרחבה לחוג פולינומים). לכן:

$$f(\Lambda) = \Lambda \Rightarrow f(E) = E \Rightarrow \tilde{E} = E \Rightarrow \beta \in E$$

■

3.1 הרחבות נורמליות

הגדרה 3.9 הרחבה אלגברית $E \geq F$ נקראת נורמלית אם לכל $\alpha \in E$, $min_F(\alpha)$ מתפצל ב־E.

דוגמאות:

1. $F \geq F$ הרחבה נורמלית.
2. $\overline{F} \geq F$ הרחבה נורמלית.
3. $|E:F| \leq 2$ הרחבה נורמלית.
4. $\mathbb{Q}\left[\sqrt[3]{2}\right] \geq \mathbb{Q}$ אינה נורמלית - כי הפולינום המינימלי הוא x^3-2 - והוא אי פריק מקריטריון איזנשטיין, ולכן לא מתפצל מעל $\mathbb{Q}\left[\sqrt[3]{2}\right]$.

משפט 3.10 תהי $E \geq F$ הרחבה סופית. התנאים הבאים שקולים:

1. E נורמלית.
2. E שדה פיצול של איזשהוא פולינום $g \in F[x]$.
3. לכל הרחבה $L \geq E$ ולכל F־איזומורפיזם $f: L \to L$ מתקיים $f(E) = E$.

לפני שנוכיח את המשפט - למה שנעזר בה:

למה 3.11 תהי $|E:F| < \infty$, ויהי $\alpha \in E$. אזי יש הרחבה סופית $L \geq E$ ופולינום $g \in F[x]$ כך ש:

1. L שדה פיצול של g.
2. לכל גורם אי פריק של g מעל F יש שורש ב־E.
3. $g(\alpha) = 0$.

הוכחה: נרחיב את $\{\alpha\}$ לבסיס $\{\alpha = \alpha_1, \alpha_2, ..., \alpha_n\}$ של $E \geq F$, ולכל $1 \leq i \leq n$ נסמן את $min_F(\alpha_i)$ הפולינום המינימלי של α_i מעל F.
נגדיר $g = \prod_{i=1}^{n} min_F(\alpha_i)$, ויהא L שדה פיצול של g מעל E. 1 במקרה זה מתקיים מההגדרה של L - אם Ω היא קבוצת שורשי g, אזי מההגדרה $L = E(\Omega)$. כמו כן $\alpha_1, ..., \alpha_n \in \Omega$, ולכן $F(\Omega) \supseteq F(\alpha_1, ..., \alpha_n) = E$, כלומר L שדה פיצול של g מעל F.
2 מתקיים כי הגורמים האי פריקים של g מעל F הם בדיוק $f_i = min_F(\alpha_i)$ לכל $1 \leq i \leq n$. אבל $f_i(\alpha_i) = 0$ מההגדרה, וכן $\alpha_i \in E$, ולכן לכל גורם אי פריק של g מעל F אכן יש שורש ב־E.
3 מתקיים ישירות גם כן, כי $\alpha = \alpha_1$, ובמקרה זה:

$$g(\alpha) = \prod_{i=1}^{n} min_F(\alpha_i) = f_1(\alpha_1) \cdot \prod_{i=2}^{n} min_F(\alpha_i) = 0 \cdot \prod_{i=2}^{n} min_F(\alpha_i) = 0$$

■

כעת, נוכיח את המשפט: **הוכחה:** $1 \Leftarrow 2$: מהלמה, קיימת הרחבה $L \geq E$ המהוה שדה פיצול לאיזשהוא $g \in F[x]$, וכן לכל גורם אי פריק של g יש שורש ב־E. אבל E נורמלית, לכן g שהגדרנו מתפצל מעל E, כלומר $E = L$.

$2 \Leftarrow 3$: נניח כי E שדה פיצול של איזשהוא פולינום $g \in F[x]$, ושוב נסמן ב־Ω את קבוצת שורשיו. אזי בפרט $E = F(\Omega)$. תהא $L \geq E$ הרחבה כלשהיא, ונביט ב־$\sigma \in Gal(L/F)$ איזומורפיזם כלשהוא. אזי, מכיוון ומקדמי g ב־F, $g = \overline{\sigma}(g)$, ולכן:

$$\sigma(\Omega) = \Omega \Rightarrow \sigma(E) = \sigma(F(\Omega)) = F(\Omega) = E$$

$3 \Leftarrow 1$: בצורה דומה למה שכבר עשינו - יהא $p \in F[x]$ פולינום אי פריק, ונניח כי $p(\alpha) = 0$ עבור איזה $\alpha \in E$. צריך להראות כי p מתפצל ב־E.

מהלמה, קיים איזהוא פולינום $g \in F[x]$ והרחבה סופית L שהיא שדה פיצול של g כך תנאי שהלמה מתקיימים.

נטען תחילה כי p איתו התחלנו מתפצל ב־L - זה נכון כי p הינו גורם אי פריק של g מתנאי 3, ולכן מתנאי 2 p מתפצל ב־L. יהא $\beta \in L$ שורש כלשהוא של p, ונרצה להראות כי $\beta \in E$.

p אי פריק מעל F, לכן קיים איזומורפיזם $f : F(\alpha) \to F(\beta)$, המתרחב לאיזומורפיזם $\tilde{f} : L \to L$, שהרי L שדה פיצול של g מעל F (ומעל $F(\alpha)$, $F(\alpha)$).

מקיום התנאי השלישי נקבל כי איזומורפיזם זה יקיים $\tilde{f}(E) = E$, אבל אנו גם יודעים כי $\tilde{f}(\alpha) = \beta$, כלומר, $\beta \in E$. הנורמליות נובעת מכאן כי β שרירותי, ולכל שורשי פולינום p הנ"ל מתקיים, כנדרש מהגדרת הנורמליות. ■

מסקנה 3.12 לכל ההרחבה סופית $E \geq F$ יש $L \geq E$ סופית כך שההרחבה $L \geq F$ נורמלית.

הוכחה: ראינו כי יש $L \geq E$ כך ש־L שדה פיצול של איזשהוא $g \in F[x]$. ■

3.2 הרחבות ספרביליות

הגדרה 3.13 נאמר כי ל־$f \in F[x]$ יש שורשים נבדלים, אם בכל הרחבה בה f מתפצל, יש לו $deg(f)$ שורשים שונים.

למה 3.14 עבור $0 \neq f \in F[x]$, התנאים הבאים שקולים:

1. ל־f יש שורשים נבדלים.
2. בכל הרחבה $E \geq F$, לכל $\alpha \in E$, $(x-\alpha)^2 \nmid f$.
3. יש הרחבה $K \geq F$ בה ל־f יש $n = deg(f)$ שורשים שונים.

הוכחה: $1 \Leftarrow 2$: תהי $E \geq F$ הרחבה, ונניח בשלילה שקיים $\alpha \in E$ כך ש־$(x-\alpha)^2 | f$. תהי $K \geq E$ הרחבה בה f מתפצל. אזי $f = (x-\alpha)^2 \cdot g$ עבור איזה g מדרגה $n-2$. במקרה זה, מספר השורשים השונים של f יהיה $n-1 \geq 1 + deg(g)$, בסתירה לנתון, שבכל הרחבה בה f מתפצל, לפולינום $deg(f)$ שורשים שונים.

$2 \Leftarrow 3$: יהא K שדה פיצול כלשהוא של F. התנאי הנתון מבטיח כי כל השורשים שונים.

$3 \Leftarrow 1$: תהא $F \leq K$ הרחבה בה ל־f יש $n = deg(f)$ שורשים שונים, ותהי K' הרחבה כלשהיא בה הפולינום יתפצל. נבחר $K \supseteq E,\ K' \supseteq E'$ שדות פיצול של f. אזי קיים F־איזומורפיזם $f : E \to E'$ בו שורשי f ב־E הולכים לשורשי f ב־E', לכן מספר השורשים קבוע. ■

29/3/2011

מסקנה 3.15 יהי $0 \neq f \in F[x],\ K \geq F$. אזי ל־$f$ יש שורשים נבדלים ב־F אמ"מ יש לו שורשים נבדלים ב־K.

הוכחה: נובעת ישירות מהשקילות בין התנאי הראשון לתנאי השלישי של הלמה. ■

הגדרה 3.16 פולינום $f \in F[x]$ נקרא ספרבילי מעל F אם לכל גורם אי פריק של f יש שורשים נבדלים.

הערה 3.17 לעיתים $f \in F[x]$ אינו ספרבילי מעל F אבל הוא כן ספרבילי מעל הרחבה $K \geq F$.
למשל, כל פולינום הוא ספרבילי מעל שדה הפיצול שלו.

למה 3.18 תהי $E \geq F$ הרחבה. אם $f \in F[x]$ ספרבילי מעל F, אזי הוא ספרבילי גם מעל E.

הוכחה: אם $p \in E[x]$ גורם אי פריק של f בחוג $E[x]$, אזי p מחלק את אחד הגורמים האי פריקים של f ב־$F[x]$. אבל, לכל גורם שכזה יש שורשים נבדלים, ולכן גם ל־p שורשים נבדלים. ■

מסקנה 3.19 אם $f \in F[x]$ בעל שורשים נבדלים וקיים $g \in F[x]$ כך ש־$g|f$, אזי גם ל־g שורשים נבדלים.

דוגמא לפולנום לא ספרבילי יהי $p > 0$ ראשוני, $E = \mathbb{F}_p(t)$, ונביט על $E[x] \ni f(x) = x^p - t$. f אי פריק לפי קריטריון איזנשטיין.
בסגור האלגברי $\overline{E}$ של E, יהא α שורש p־אי של t, כלומר $\alpha^p = t$. אזי:

$$(x-\alpha)^p = x^p - \binom{p}{1} x^{p-1}\alpha + \binom{p}{2} x^{p-2}\alpha^2 + ... - \alpha^p = x^p - \alpha^p = f(x)$$

כאשר כל הביטויים חוץ מהראשון והאחרון מתאפסים כיוון והמציין של השדה הוא p, והוא מחלק את כל המקדמים של אותם האיברים.

משפט 3.20 אם $charF = 0$ או F סופי, אזי כל פולינום מעל F הוא ספרבילי.

הוכחה: בתרגול. מקווה שאספיק להביא אותה לכאן. ■

הגדרה 3.21 תהא $E \geq F$ הרחבת שדות. $\alpha \in E$ נקרא ספרבילי אם $min_F(\alpha)$ ספרבילי ($\Leftrightarrow$ ל־$min_F(\alpha)$ שורשים נבדלים).

הגדרה 3.22 $E \geq F$ תקרא הרחבה ספרבילית אם כל איברי E ספרביליים מעל F.

מסקנה 3.23 תהי $E \geq F$ הרחבה, ויהי $E \geq K \geq F$ שדה ביניים. אם $E \geq F$ ספרבילית, אזי גם $E \geq K,\ K \geq F$ ספרביליות.

הוכחה: ברור מההגדרה כי $K \geq F$ ספרבילית, כי $E \supseteq K$.
יהא $\alpha \in E$. אזי $min_K(\alpha) | min_F(\alpha)$. נתון כי ל־$min_F(\alpha)$ שורשים נבדלים, ולכן גם ל־$min_K(\alpha)$, כלומר α ספרבילי מעל K. ■

4/4/2011

משפט 3.24 תהי $E \geq F$ הרחבה סופית . אזי, התנאים הבאים שקולים:

1. $E \geq F$ הרחבת גלואה.
2. $E \geq F$ ספרבילית ונורמלית.
3. E שדה פיצול של איזה פולינום ספרבילי.

כהרגלנו, תחילה נוכיח למה שבעזרתה נוכיח את המשפט הנ"ל:

למה 3.25 יהי E שדה, $G \leq Aut(E)$, ונסמן $\Lambda = G.\alpha = \{\sigma(\alpha) | \sigma \in G\}$, $F = Fix(G)$. אם Λ סופית, אזי α אלגברי מעל F, וכן $f = min_F(\alpha)$ מקיים:

1. ל־f שורשים נבדלים.
2. f מתפצל ב־E.
3. Λ היא קבוצת השורשים של f.
4. $deg(f) = |\Lambda|$.

הערה 3.26 אנו מניחים כי G חבורה הפועלת על קבוצה כלשהיא. אזי לכל α בקבוצה, $\Lambda = G \cdot \alpha = \{\sigma(\alpha) | \sigma \in G\}$. מההגדרה של G שלנו, לכל $\tau \in G$:

$$\tau\Lambda = \{\tau\sigma(\alpha) | \sigma \in G\} = \Lambda$$

ולכן G פועלת בתמורות על Λ!

הוכחה: נגדיר $E[x] \ni f(x) = \prod_{\beta\in\Lambda}(x-\beta)$.
נראה כי $f \in F[x]$, וכי $f = min_F(\alpha)$. מכיוון ש־$F = Fix(G)$, מספיק להראות כי לכל $\sigma \in G$, $\overline{\sigma}f = f$ כדי להראות כי $f \in F[x]$. זה מתקיים, כי:

$$\overline{\sigma}(f(x)) = \overline{\sigma}\left(\prod_{\beta\in\Lambda}(x-\beta)\right) = \prod_{\beta\in\Lambda}(x-\sigma(\beta)) = \prod_{\beta\in\Lambda}(x-\beta) = f(x)$$

ברור כי $f(\alpha) = 0$ מההגדרה (כי העתקת הזהות מבטיחה כי $\alpha \in \Lambda$).
אזי, על מנת להראות כי $f = min_F(\alpha)$, נותר רק להראות כי f אי פריק. נניח בשלילה כי קיים $F[x] \ni g | f$ לא טריוויאלי לא הפיך. עד כדי כפל בסקלר g מתוקן, ולכן:

$$g(x) = \prod_{\beta\in\Lambda'}(x-\beta)$$

עבור תת קבוצה ממש $\Lambda' \lneq \Lambda$.
יהיו $\beta \in \Lambda'$, $\delta \in \Lambda\backslash\Lambda'$. אזי, מצד אחד, לכל $\sigma \in G$, $\sigma(\beta)$ הוא שורש של g. כלומר $\sigma(\beta) \in \Lambda'$. מצד שני, יש $\sigma \in G$ כך ש־$\sigma(\beta) = \delta$ ־ סתירה!
לכן $f \in min_F(\alpha)$. כל שאר התנאים נובעים מהגדרה שלנו של f. ■

כעת, נוכיח את המשפט: **הוכחה:** $2 \Leftarrow 1$: תהי $E \geq F$ הרחבת גלואה. לכל $\alpha \in E$ הפולינום המינימלי מקיים את תנאי הלמה, ולכן ספרבילי, ובפרט $E \geq F$ הרחבה ספרבילית.
כמו כן, אם $f \in F[x]$ פולינום אי פריק עם שורש, אזי הוא מתפצל (לפי הלמה) כי הוא הפולינום המינימלי של עצמו. לכן $E \geq F$ נורמלית.

הערה 3.27 כאשר $E \geq F$ אלגברית (או סופית), אזי $|G.\alpha| < \infty$ לכל $\alpha \in G$, כי $G.\alpha$ מוכל בקבוצת השורשים של $min_F(\alpha)$.

$2 \Leftarrow 3$: מניחים כי $E \geq F$ סופית ספרבילית ונורמלית. יהא $\alpha_1, ..., \alpha_n$ בסיס ל־E מעל F, ונגדיר:

$$g = \prod_{i=1}^{n} min_F(\alpha_i)$$

$min_F \alpha_i$ הוא אי פריק בעל שורש ב־E, ו־$E \geq F$ נורמלית מהנתון, ועל כן הוא מתפצל, ולכן, כמכפלה של פולינומים מתפצלים, גם g מתפצל. $E \geq F$ גם ספרבילית, ולכן $min_F(\alpha_i)$ ספרבילי, ולכן g ספרבילי.

קיבלנו כי g ספרבילי ומתפצל, אבל שורשיו פורשים את E, ולכן אין שדה קטן יותר מעליו הוא מתפצל - לכן E שדה הפיצול של g.

$3 \Leftarrow 1$: שוב משתמש בלמה, וכן גם באינדוקציה על מעלת ההרחבה -

בסיס האינדוקציה: ברור כי הטענה נכונה כאשר ההרחבה ממעלה 1, כלומר כאשר $E = F$.

צעד האינדוקציה: נסמן $K = Fix(G)$, ונרצה להוכיח כי $K = F$ על מנת שההרחבה תהיה גלואה.

נניח כי E שדה פיצול של פולינום ספרבילי $g \in F[x]$, וכן נניח כי $E \gneq F$.

למה 3.28 G איננה טריוויאלית. **הוכחה:** E כאמור שדה פיצול של g ספרבילי, ולכן יש לו לפחות שני שורשים שונים - $\alpha \neq \beta$. אזי $F[\alpha] \simeq F[\beta]$, והאיזומורפיזם ביניהם מתרחב ל־F אוטומורפיזם של E - העתקה זו היא ב־G, ואינה טריוויאלית (בפרט β עובר ל־α). ■

על כן, בפרט $E \gneq K$, ומכיוון ששורשי g פורשים את E, קיים $\alpha \in E/K$ כך ש־$g(\alpha) = 0$.

$E \geq F[\alpha] \gneq F$, ובפרט $|E : F| > |E : F[\alpha]|$, וזוהי בהכרח עדיין הרחבת פיצול של g ולכן מהנחת האינדוקציה , ולכן $E \geq F[\alpha]$ הרחבת גלואה ו־$G \leq (Gal(E/F[\alpha])$, ומתכונת גלואה $K = Fix(G) \subseteq F[a] = Fix(Gal(E/F[\alpha]))$. כמו כן, בוודאי ש־$F \subseteq K$.

על מנת להראות כי $K = F$, מספיק להראות כי

$$|F[\alpha] : F| = |F[\alpha] : K|$$

ולשם כך מספיק להראות כי $min_F(\alpha)$ הוא אי פריק מעל K - כי אז זה יהיה הפולינום המינימלי גם מעל K, ומכיוון וההרחבה פשוטה, דרגתה שווה לדרגת הפולינום המינימלי - ומשיוויון הזה נסיים.

נסמן $f = min_F \alpha$, $k = min_K \alpha$, וכן נסמן את קבוצות השורשים ב־Λ_K, Λ_F בהתאמה. f, k פולינומים מינימליים של α, וכן $g(\alpha) = 0$, ולכן $k, f | g$ כאשר g ספרבילי, ולכן גם הם ספרביליים. לכן $deg(f) = |\Lambda_F|$, $deg(g) = |\Lambda_K|$, כלומר יספיק לנו להוכיח שיוויון בין קבוצות השורשים.

מההכלה, $k|f$ ולכן $\Lambda_k \subseteq \Lambda_f$. נוכיח את הכיוון השני - יהי β שורש של f, אי פריק ולכן יש איזומורפיזם $\phi : F[\alpha] \to F[\beta]$, וכיוון ו־$E$ שדה פיצול של g מעל שניהם ו־g, $\phi(g) = g$, אזי הוא מתרחב ל־F איזומורפיזם של E המקיים $\tilde{\phi}(\alpha) = \beta$. זהו כאמור F איזומורפיזם, לכן $\phi \in G$, ולכן בפרט $\beta \in G.\alpha$. מהלמה הקודמת $\Lambda_K = g.\alpha$, ולכן $\beta \in \Lambda_K$, ולכן קיבלנו שיוויון.

■

מסקנה 3.29 אם $E \geq F$ הרחבת גלואה, אזי לכל שדה ביניים $F \leq K \leq E$, $K \leq E$ הרחבת גלואה.

הוכחה: $E \geq F$ גלואה ולכן נורמלית וספרבילית. כשדה ביניים, $E \geq K$ נורמלית וספרבילית, ולכן $E \geq K$ גלואה. ■

3.3 החבורה המתאימה

למה 3.30 לכל הרחבה סופית $E \geq F$, $Gal\left(E/F\right)$ היא חבורה סופית.

הוכחה: יהא $\{\alpha_1, ..., \alpha_n\}$ בסיס ל־E מעל F.
ניקח $f = \prod_{i=1}^{n} min_F\left(\alpha_i\right)$, ונסמן $\Lambda = \{\alpha \in E | f\left(\alpha\right) = 0\}$. אזי $|\Lambda| \leq deg\left(f\right)$.
כיוון ש־$E = F\left[\alpha_1, ..., \alpha_n\right] \subseteq F\left[\Lambda\right]$, מלמה קודמת ההומומורפיזם $Gal\left(E/F\right) \to Sym\left(\Lambda\right)$ חח"ע. לכן אם $|\Lambda| = m$ מספר סופי, אזי $m \geq |Gal\left(E/F\right)|$ סופי גם כן. ■

למה 3.31 לכל הרחבה ספרבילית סופית $E \geq F$ יש הרחבה סופית $L \geq E$ כך ש־$L \geq F$ גלואה.

הוכחה: יהא $\alpha_1, ..., \alpha_n$ בסיס ל־E מעל F. נגדיר $f = \prod_{i=1}^{n} min_F\left(\alpha_i\right)$. נגדיר את L להיות שדה הפיצול של f. כיוון ש־E ספרבילית אזי f ספרבילי, כלומר L שדה פיצול של פולינום ספרבילי, ולכן $L \geq F$ גלואה. ■

3.3.1 משפט האיבר הפרימיטיבי (ומשפטים הנובעים ממנו)

משפט 3.32 כל הרחבה סופית ספרבילית היא פשוטה.

הוכחה: ראינו ממשפט ארטין כי מספיק שנוכיח כי מספר שדות הביניים הוא סופי.
תהא $E \geq F$ הרחבה סופית ספרבילית. נבחר L הרחבה סופית כך ש־$L \geq F$ גלואה (לפי הלמה הקודמת - קיימת אחת כזו). אזי, קיימת העתקה חח"ע ועל בין קבוצת שדות הביניים, לבין $\mathcal{G}_0$ - קבוצת תתי החבורות של $Gal\left(L/F\right)$. אבל, $Gal\left(L/F\right)$ סופית, ולכן גם $\mathcal{G}_0$ סופית - ועל כן, קבוצת שדות הביניים סופית, ולכן $\{K | F \leq K \leq E\} \subseteq \{K | F \leq K \leq L\}$ סופית. לכן, $E \geq F$ הרחבה פשוטה, כלומר, קיים $\alpha \in E$ כך ש־$E = F\left(\alpha\right)$. ■

כמסקנה ממשפט האיבר הפרמיטיבי, נקבל את המשפט הבא:

משפט 3.33 תהי $E \geq F$ הרחבה סופית. אזי, $|Gal\left(E/F\right)|$ מחלקת את מעלת ההרחבה, וקיים שיוויון אמ"מ ההרחבה היא גלואה.

הוכחה: נניח ראשית כי $E \geq F$ הרחבת גלואה. בפרט היא ספרבילית, לכן ממשפט האיבר הפרימיטיבי יש $\alpha \in E$ כך ש־$E = F\left(\alpha\right)$.
ממשפט קודם, היא גם נורמלית, ולכן הפולינום המינימלי $min_F\left(\alpha\right)$ מתפצל. ראינו כי $deg\left(min_F\left(\alpha\right)\right) = |E : F| = d$, כי $min_F\left(\alpha\right)$ ספרבילי, על כן יש לו d שורשים שונים.
נסמן ב־Λ את קבוצת שורשי $min_F\left(\alpha\right)$. אזי, $|\Lambda| = d$, ולכל $\beta \in \Lambda$ ה־F־איזומורפיזם $F\left[\alpha\right] \to F\left[\beta\right]$ מתרחב ל־F איזומורפיזם בין שדה הפיצול (למעשה $F\left[\alpha\right]$ הוא שדה הפיצול). כלומר, $Gal\left(E/F\right)$ פועלת טרנזיטיבית על Λ.

אבל, אם $\sigma(\alpha)=\tau(\alpha)$, אז $\sigma^{-1}\tau(\alpha)=\alpha$, כלומר $\sigma^{-1}\tau=id$, כי α יוצר את E. לכן, $Gal(E/F)$ פועלת טרנזיטיבית חופשית (ללא מייצבים) על Λ, ולכן $|Gal(E/F)|=|\Lambda|=d$.[12]

תהא עתה $E\geq F$ הרחבה סופית כלשהיא. נסמן $K=Fix(Gal(E/F))$. אזי, E/K היא הרחבת גלואה, ואם נסמן $G=Gal(E/K)$, אזי ממה שראינו מעלה, $|G|=|E:K|$, לכן $|G|\,||E:F|$, שהרי:

$$|E:F|=|E:K|\cdot|K:F|$$

לכן $|G|\,||E:F|$, וקיים שיוויון אמ"מ $K=F$, כלומר אמ"מ $E\geq F$ גלואה. ■

באופן כללי, כאשר חבורה G פועלת טרנזיטיבית על קבוצה X, וכן $\alpha\in X$, $G_\alpha=\{\sigma\in G|\sigma(\alpha)=\alpha\}$ חבורת המייצב, אזי קיימת התאמה חח"ע ועל טבעית בין X לבין G/G_α הנתונה ע"י $\sigma.G_\alpha\to\sigma(\alpha)$. בפרט $|G:G_\alpha|=|X|$. אזי, אם G_α טריוויאלית, נקבל $|G|=|X|$.

5/4/2011

משפט 3.34 יהא E שדה, $G\leq Aut(E)$ חבורה סופית, ויהא $F=Fix(G)$. אזי:

1. $|E:F|=|G|$.
2. $G=Gal(E/F)$.
3. $E\geq F$ הרחבת גלואה.

הערה 3.35 1 ו־2 גוררים את 3 מהמשפט הקודם, כי $2+1$ גוררים:

$$|E:F|=|Gal(E/F)|$$

לכן E/F הרחבת גלואה.
תרגיל: $3+1$ גוררים את $2+2$, $3+1$ גוררים את 1.

הוכחה: לכל $\alpha\in E$, יהא $\Lambda_\alpha=G.\alpha=\{\sigma(\alpha)\,|\sigma\in G\}$. אזי Λ_α סופית (כי G סופית), וכן $|\Lambda_\alpha|\leq|G|$.
אזי, לפי למה קודמת, הפולינום $f_\alpha(x)=\prod_{\beta\in\Lambda_\alpha}(x-\beta)$ הוא הפולינום המינימלי המתוקן של α מעל F, יש לו שורשים נפרדים ועל כן ספרבילי, וכן מתפצל מעל E. זה נכון כאמור לכל $\alpha\in E$, ולכן ההרחבה $E\geq F$ נורמלית וספרבילית[13]. נשים לב כי אין זה אומר שהיא גלואה - שכן לא ידוע לנו כי $E\geq F$ סופית!
בנוסף, לכל $\alpha\in E$:

$$|F(\alpha):F|=deg(f_\alpha)=|\Lambda_\alpha|\leq|G|$$

נבחר $\alpha\in E$ כך ש־$|F(\alpha):F|=deg(f_\alpha)$ מקסימלי.

---

[12] מדוע?
ממשפט ממבנים 1 - המשוואה החיבורית של G הינה משוואה הנותנת את גודלה של קבוצה שמבוצעת עליה פעולה. על פי המשוואה, הגודל שווה לסכום גדלי מחלקות הצמידות\המסלולים השונים של הפעולה, ועוד מספר האיברים שפעולה משאירה במקום - המייצבים. כאן הפעולה טרנזיטיבית - כלומר, יש מסלול אחד באורך d, וכן ראינו כי אין מייצבים. לכן, גודלה של G שווה בדיוק לאורך המסלול.
[13] גם אלגברית, אבל נשים ♡ כי אלגברי לא שקול לסופי - לדוגמא, הסגור האלגברי של $\mathbb{Q}$ ב־$\mathbb{C}$ הוא כאמור לא סופי, אך אלגברי.

טענה 3.36 $E = F(\alpha)$.

הוכחה: נניח בשלילה שיש $\beta \in E \backslash F(\alpha)$. אזי:

$$F(\alpha,\beta) \gneq F(\alpha) \Rightarrow |F(\alpha):F| < |F(\alpha,\beta):F| < \infty$$

כלומר, קיבלנו כי ההרחבה $F(\alpha,\beta) \geq F$ סופית. מצד שני, אנו יודעים כי $E \geq F$ ספרבילית, $F(\alpha,\beta) \geq F$ ספרבילית. לכן, ממשפט האיבר הפרימיטיבי יש $\gamma \in F(\alpha,\beta)$ כך ש־$F(\gamma) = F(\alpha,\beta)$, לכן:

$$deg(f_\gamma) = |F(\gamma):F| = |F(\alpha,\beta):F| > |F(\alpha):F| = deg(f_\alpha)$$

בסתירה להנחת המקסימליות של $deg(f_\alpha)$. ■

טכנית, נוכל לעצור כבר כאן - מכיוון ואנחנו יודעים כעת כי E הרחבה סופית, וכן מההתחלה היא נורמלית וספרבילית, ולכן גלואה, ולכן בפרט $F = Fix(G) = Fix(Gal(E/F))$, כלומר $G = Gal(E/F)$, ולכן מהמשפט הקודם נקבל את נכונות התנאי הראשון.
אבל המשכנו בכיתה, ולכן אביא כאן גם את ההמשך:
כמו כן, ברור כי $G \subseteq Gal(E/F)$. קיבלנו בסה"כ:

$$|E:F| = |F(\alpha):F| = deg(f_\alpha) \leq |G| \leq |Gal(E/F)| \leq |E:F|$$

לכן $|Gal(E/F)| = |E:F|$, כלומר $E \geq F$ גלואה, וכן $|Gal(E/F)| = |G|$, ולכן (מכיוון והיא חלקית לה) נקבל שיוויון. ■

מסקנה 3.37 בכל הרחבה סופית $E \geq F$, $\mathcal{G}_0 = \mathcal{G}$, כאשר $\mathcal{G}$ הוא אוסף תתי החבורות של חבורת גלואה של E/F, ו־$\mathcal{G}_0$ אוסף החבורות המקיימות $G = Gal(E/Fix(G))$.

אתמול ראינו כי עבור הרחבת גלואה, $\mathcal{F}_0 = \mathcal{F}$. כעת ראינו כי בכל הרחבה סופית, $\mathcal{G}_0 = \mathcal{G}$, ובעבר ראינו כי קיימת התאמה חח"ע ועל בין $\mathcal{G}_0$ לבין $\mathcal{F}_0$. כעת, נוכיח משפט:

3.3.2 המשפט היסודי של חבורת גלואה

משפט 3.38 תהא $E \geq F$ הרחבת גלואה. נסמן $G = Gal(E/F)$, $\mathcal{F}$ קבוצת שדות הביניים בין F ל־E, ו־$\mathcal{G}$ קבוצת תת החבורות H המקיימות $H \leq Gal(E/F)$. אזי:

1. קיימת התאמה $f : \mathcal{G} \to \mathcal{F}$ המתאימה את G ל־$Fix(G)$, וכן קיימת התאמה $g : \mathcal{F} \to \mathcal{G}$ המתאימה את K ל־$Gal(E/K)$. התאמות אלו חח"ע, על והופכיות זו לזו, וכן הופכות את סדר ההכלה.
2. אם $g(K) = H$ (כלומר $f(H) = K$), אזי $|E:K| = H$, $|K:F| = |G:H|$, ובפרט $|E:F| = |G|$.
3. אם $g(K) = H$, $\sigma \in Gal(E/F)$, אזי $g(\sigma(K)) = \sigma^{-1}H\sigma$, וכן $H \lhd G$ אמ"מ $K \geq F$ הרחבת גלואה, ובמקרה זה $Gal(K/F) \simeq G/H$.

הוכחה: את שני הסעיפים הראשונים ראינו בעבר - רק נסביר מדוע $|K:F| = |G:H|$:

$$|E:F| = |E:K| \cdot |K:F| \Rightarrow |E:F|/|E:K| = |K:F|$$

ומצד שני:

$$|E:F|=G,\ |E:K|=H \Rightarrow {}^{|E:F|}/_{|E:K|}={}^{|G|}/_{|H|}=|G:H|$$

כפי שרצינו!

נוכיח אם כך את 3 ונסיים.

$\tau \Leftrightarrow \tau \in g\left(\sigma\left(K\right)\right) \Leftrightarrow \sigma\left(K\right)$ מקבע כל איבר $\sigma^{-1}\tau\sigma$ מקבע כל איבר ב־$K \Leftrightarrow$ $H=g\left(K\right) \ni \sigma^{-1}\tau\sigma$, ומכיוון והוכחה זו דו כיוונית, נקבל הכלה משני הצדדים, ועל כן שיוויון.

$E \geq F$ גלואה ולכן בפרט ספרבילית, וראינו שלכן כל הרחבת ביניים $K \geq F$ ספרבילית, ולכן $K \geq F$ גלואה אמ"מ היא גם נורמלית.

בכיוון ראשון, אם היא גלואה אז היא נורמלית, אזי ממשפט שהוכחנו לגבי הרחבות נורמליות, לכל $\sigma \in Gal\left({}^{E}/_{F}\right)$, $\sigma\left(K\right)=K$, ואז נקבל:

$$\forall \sigma \in Gal\left({}^{E}/_{F}\right)\ \ \sigma^{-1}H\sigma=g\left(\sigma\left(K\right)\right)=g\left(K\right)=H$$

כלומר $H \lhd G$.

בכיוון השני, נניח $H \lhd G$, ונניח בשלילה כי $K \geq F$ לא נורמלית. אזי ישנו $\alpha \in K$ כך שהפולינום המינימלי שלו מעל F לא מתפצל ב־K. לכן יש לו שורש $\beta \in E \backslash K$, ואז קיימת איזושהיא העתקה $\sigma \in Gal\left({}^{E}/_{F}\right)$ שמחליפה בינו לבין שאר השורשים. אבל אז נקבל כי $\beta \in \sigma\left(K\right)$ ולא ב־$H=g\left(K\right)$, כלומר $K \neq \sigma\left(K\right)$, בסתירה לנורמליות של H ב־G, ממנה נקבל:

$$g\left(K\right)=H=\sigma^{-1}H\sigma=g\left(\sigma\left(K\right)\right) \Rightarrow K=\sigma\left(K\right)$$

כשהסתירה מתקבלת כי g חח"ע. לכן קיבלנו כי $K \geq F$ גלואה אמ"מ $H \lhd G$.

נגדיר את $\varphi : G \to Gal\left({}^{K}/_{F}\right)$ להיות העתקת הצמצום ־ כלומר, ההעתקה מצמצמת כל $\sigma \in G$ ל־$\sigma|_{E}$. היא מוגדרת היטב, שכן $\sigma\left(K\right)=K$. כמו כן, היא הומומורפיזם ישירות מהגדרתה. הגרעין של ההעתקה הוא $H=Gal\left({}^{E}/_{K}\right)$, שכן רק כאשר מצמצמים את ההעתקות הללו מקבלים את הזהות. נראה כי ההעתקה היא על משיקולי עוצמה: H נורמלית, ${}^{K}/_{F}$ גלואה, ונקבל:

$$|Im\varphi|=\frac{|G|}{|H|}=\frac{|E:F|}{|E:K|}=|K:F|=|Gal\left({}^{K}/_{F}\right)|$$

לכן, ממשפט ממבנים 1 על הומומורפיזמים בין חוגים, נקבל כי:

$$im\varphi \simeq {}^{G}/_{ker\varphi} \Rightarrow Gal\left({}^{K}/_{F}\right) \simeq {}^{G}/_{H}$$

■

תרגיל: $F=\mathbb{Q}$, E שדה הפיצול של $p\left(x\right)=x^4-2$. הראו כי $|E:F|=8$, $E \geq F$ הרחבת גלואה. זהו את G.

משפט 3.39 יהיו $F \leq E \leq K$ שדות, $E \geq F$ הרחבת גלואה, $F \leq L \leq K$ שדה ביניים כך שהשדה הקטן ביותר המכיל את E, L ־ נסמנו ב־ $\langle E, L\rangle$, הוא K.

אזי, ${}^{K}/_{L}$ היא הרחבת גלואה, וכן:

$$Gal\left({}^{K}/_{L}\right) \simeq Gal\left({}^{E}/_{E\cap L}\right)$$

ובפרט $|K:L|=|E:E\cap L|$.

הוכחה: $E \geq F$ הרחבת גלואה, לכן קיים פולינום $f \in F[x]$ ספרבילי כך ש־E שדה הפיצול של f, לכן הוא גם מתפצל ב־K. בנוסף, אם Λ קבוצת שורשי f ב־E, אזי $L(\Lambda) \supset F(\Lambda) = E$.

$L(\Lambda) \supseteq E, L$, והוא הקטן ביותר המכיל את שניהם - כי הוא חייב להכיל את L ואת השורשים של f ב־E. לכן $L(\Lambda) = K$, כלומר K הוא שדה הפיצול של f מעל L, לכן $K \geq L$ הרחבת גלואה.

תהי $\sigma \in Gal(K/L)$. אזי σ מקבעת את L ולכן את F. $E \geq F$ גלואה ולכן בפרט נורמלית, לכן (מהמשפט אודות הרחבות נורמליות) $\sigma(E) = E$. לכן, הצמצום הוא הומומורפיזם:

$$Gal(K/L) \xrightarrow{r} Gal(E/E\cap L)$$

אבל אם $r(\sigma) = id_E$ אז σ מקבעת את כל איברי E, ובפרט את כל איברי Λ. אבל, $K = L(\Lambda)$, ולכן $\sigma = id_K$, כלומר r חח"ע. נותר להראות כי r היא על.

נסמן $l = |E : E \cap L|$, ויהא α יוצר של E מעל $E \cap L$ (קיים ממשפט האיבר הפרימיטיבי). אזי $L(\alpha) \supseteq E, L$, ולכן $L(\alpha) = K$. לכן, קיימות חזקות $\alpha^{k_1}, \alpha^{k_2}, ..., \alpha^{k_t}$ כך ש־$t = |K : L|$, המהוות בסיס ל־K מעל L, ולכן הם בת"ל מעל L, ולכן בפרט גם מעל $E \cap L$

בפרט, $t \leq d = dim_{E\cap L} E$, ולכן:

$$|K : L| = t \geq |E : E \cap L|$$

ובעצם הראנו כאן הוכחה נוספת לצד הראשון. אין ממש שימוש לזה, כנראה שצחיק התברבר עם עצמו.

נסמן את התמונה של r ב־H.

מצד אחד, ברור כי $E \cap L \subseteq FixH$. כמו כן, $FixH \subseteq E$.

מצד שני, אם $\sigma \in H$, אזי היא צמצום של $\tilde{\sigma} \in Gal(K/L)$, כלומר מקבעת את L, ולכן בפרט $FixH \subseteq L$. קיבלנו:

$$E \cap L \subseteq FixH \subseteq E, L \Rightarrow E \cap L \subseteq FixH \subseteq E \cap L$$

ולכן $FixH = E \cap L$.

אנו יודעים כי $E \geq E \cap L$ גלואה, כי $E \cap L$ שדה ביניים בין E ל־F. אזי, $H = Gal(E/E\cap L)$, ולכן, מהמשפט היסודי, $Fix(Gal(E/E\cap L)) = E \cap L = FixH$ - כלומר, התמונה של ההעתקה היא בדיוק כל $Gal(E/E\cap L)$, ולכן ההעתקה היא גם על, כנדרש. ■

3.4 הרחבות ציקלוטומיות

הגדרה 3.40 שורש יחידה $\alpha \in F$ הוא איבר המקיים $\alpha^n = 1$ לאיזה n.

לדוגמא: ב־$\mathbb{C}$, שורשי היחידה מסדר n הם מהצורה $\alpha = e^{\frac{2\pi ik}{n}}$.

הגדרה 3.41 α נקרא n־פרימיטיבי אם $\alpha^m \neq 1$ לכל $m < n$.

לדוגמא: ב־$\mathbb{C}$, $\alpha = e^{\frac{2\pi ik}{n}}$ שורש יחידה פרימיטיבי $\Leftrightarrow (k, n) = 1$.

למה 3.42 יהי F שדה, $n \in \mathbb{N}$. אזי, שורשי היחידה ה־n־אים מהווים חבורה כפלית ציקלית מסדר המחלק את n, ושווה לו $\Leftrightarrow$ יש שורש n־פרימיטיבי.

הוכחה: אם $\alpha^n = 1 = \beta^n$, אז $(\alpha\beta)^n = \alpha^n\beta^n = 1$ מקמוטטיביות, ובנוסף, $\left(\frac{1}{\alpha}\right)^n = \frac{1}{\alpha^n} = 1$, ולכן הם מהווים חבורה.

כל שורש יחידה n־י הוא שורש של הפולינום $x^n = 1$, ולכן יש מספר סופי של כאלה. לכן זו חבורה סופית ב־$F*$, ולכן ציקלית.

על כן, יש $\alpha \in F*$ כך ש־$\langle\alpha\rangle$ היא קב' כל שורשי היחידה ה־n־אים. אם הסדר של α הוא k, נרשום $n = ak + b$, כאשר $0 \leq b < k$. אזי:

$$1 = \alpha^n = \left(\alpha^k\right) \cdot \alpha^b = \alpha^b$$

ולכן $b = 0$. כלומר, $k|n$, ויש שיוויון אמ"מ α n־פרימיטיבי. ■

מסקנה 3.43 נניח $\alpha \in F$ שורש יחידה n־פרימיטיבי. אזי:

- כל שורש יחידה n־י הוא מהצורה a^k לאיזה $1 \leq k \leq n$.
- α^k הוא שורש יחידה n־פרימיטיבי אמ"מ $(k, n) = 1$.
- יש בדיוק $\varphi(n)$ (פונקציית אוילר) שורשי יחידה n־פרימיטיביים.

הוכחה: תרגיל.

הערה שלי: שני הסעיפים הראשונים נובעים ישירות מההגדרה. השלישי נובע מהגדרת פונקציית אוילר (באדיבות ויקיפדיה): "$\varphi(n)$ שווה למספר המספרים הטבעיים הזרים ל־ n ואינם גדולים ממנו" - ואז הסעיף השלישי נובע ישירות מהסעיף השני. ■

למה 3.44 יהי F שדה, $n \in \mathbb{N}$. אזי יש ל־F הרחבה E עם שורש יחידה $\alpha \in E$ n־פרימיטיבי $\Leftrightarrow char(F) \nmid n$, ובמקרה זה $F(\alpha)$ הוא שדה הפיצול של הפולינום $x^n - 1$, ובפרט נקבע ביחידות עד כדי איזומורפיזם.

הוכחה: אם $char(F) = p|n$, אז נרשום $n = mp$, ואז $x^n - 1 = (x^m - 1)^p$, ולכן לפולינום זה יש לכל היותר m שורשים, ולכן אין שורש n־פרימיטיבי.

אחרת, אם $char(F) = p \nmid n$, אזי (בעזרת קריטריון מהתרגול), לנגזרת של הפולינום:

$$(x^n - 1)' = nx^{n-1}$$

יש שורש יחיד שהוא 0, ולכן $(x^n - 1)'$ זר ל־$x^n - 1$, ולכן לפולינום זה שורשים נבדלים. לכן, אם E שדה הפיצול שלו, אזי ב־E יש n שורשים, ואלו מהווים חבורה ציקלית, ולכן יוצרה הוא שורש n־פרימיטיבי. ■

הערה 3.45 בפרט, הנאמר מעלה נכון כאשר $\mathrm{charF} = 0$ לכל $n \in \mathbb{N}$.

2/5/2011

הערה 3.46 מעתה נעבוד מעל $\mathbb{C}$.

הגדרה 3.47 $\mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right) = \mathbb{Q}_n$ - אם נוסיף כל שורש יחידה n פרימיטיבי מעל $\mathbb{C}$, עדיין נקבל את אותו השדה.

הגדרה 3.48 הפולינום הציקלוטומי מסדר n מוגדר להיות:

$$\phi_n(x) = \prod_{\substack{1\le k<n \\ (k,n)=1}} \left(x - e^{\frac{2\pi i k}{n}}\right) = \prod_{\alpha\in\mathbb{C} \text{ is an nth root of unity}} (x-\alpha)$$

הערה 3.49 $deg\phi_n = \varphi(n)$.

דוגמאות:

$$\begin{aligned}
&\phi_1(x) = x-1 \\
&\phi_2(x) = x+1 \\
&\phi_3(x) = \left(x - e^{\frac{2\pi i}{3}}\right)\left(x + e^{\frac{2\pi i}{3}}\right) = x^2+x+1 \\
&\phi_4(x) = (x+i)(x-i) = x^2+1
\end{aligned}$$

למה 3.50 $x^n - 1 = \prod_{\substack{1\le k\le n \\ k|n}} \phi_k(x)$.

הוכחה: נשים לב כי x^n-1 מתפצל ל:

$$\prod_{m=1}^{n} \left(x - e^{\frac{2\pi i m}{n}}\right)$$

שהרי איברים אלו הם שורשי x^n-1, מהגדרתם. נשים לב כי כל שורש יחידה המופיע בביטוי הוא k פרימיטיבי עבור איזה k, לכל $k|n$, ורק לכאלה, וכל שורשי היחידה ה־k פרימיטיביים מופיעים במכפלה לעיל. מכאן נובעת הלמה ישירות. ■

מסקנה 3.51 $n = \sum_{k|n} \varphi(k)$.

הוכחה: משווים את הדרגות של הפולינומים בצידי המשוואה בלמה האחרונה. ■

מסקנה 3.52 $Z[x] \ni \phi_n(x)$, וכן הוא פולינום מתוקן.

הוכחה: באינדוקציה על n:
בסיס: עבור $n=1$, $\phi_1(x) = x-1 \in \mathbb{Z}[x]$.
נניח כי הטענה נכונה לכל $k<n$, ונוכיח אותה עבור n. מהלמה:

$$x^n - 1 = \prod_{\substack{1\le k\le n \\ k|n}} \phi_k(x) = \phi_n(x) \cdot \prod_{\substack{1\le k<n \\ k|n}} \phi_k(x)$$

הביטוי הימני מתוקן וב־$\mathbb{Z}[x]$, מהנחת האינדוקציה. x^n-1 מתוקן, ולכן, בעזרת חילוק ארוך, נקבל כי הפולינום $\phi_n(x)$ מתוקן, וכן כי הוא ב־$\mathbb{Z}[x]$, כנדרש. ■

דוגמא:

- אם p ראשוני, אז:

$$x^p-1=\phi_p(x)\cdot\phi_1(x)$$
$$\Rightarrow \phi_p(x)=\frac{x^p-1}{\phi_1(x)}=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+...+1$$

- עבור $n=6$:

$$\phi_6(x)=\frac{x^6-1}{\phi_1(x)\cdot\phi_2(x)\cdot\phi_3(x)}=x^2-x+1$$

סימון: נסמן ב־$U_n=(\mathbb{Z}/(n))^*$ את חבורת ההפיכים בחוג $\mathbb{Z}/(n)$. זוהי חבורה אבלית, וכן $|U_n|=\varphi(n)$ ־ שהרי אלו בדיוק כל ההפיכים.

למה 3.53 $U_n\simeq Aut(\mathbb{Z}/(n))$, ובפרט $Aut(\mathbb{Z}/(n))$ היא אבלית, ואם n ראשוני, אזי היא ציקלית.

הוכחה: יהי $\varphi\in Aut(\mathbb{Z}/(n))$. נגדיר העתקה שמתאימה למספר $k\in U_n$ העתקה המקיימת: $\varphi(1)=k$. אזי, לכל $m<n$:

$$\varphi(m)=\varphi\left(\overbrace{1+1+...+1}^{\text{m times}}\right)=\varphi(1)+\varphi(1)+...+\varphi(1)=k+k+...+k=mk$$

מכיוון ש־1 יוצר את $\mathbb{Z}/(n)$ כחבורה חיבורית, גם $\varphi(1)=k$ חייב ליצור אותה, לכן $(k,n)=1$ ־ ולכן החבורה נוצרת בדיוק על ידי ההפיכים המקיימים תנאי זה.
מצד שני, $\varphi(1)$ קובע את φ, ולכן כל k מגדיר העתקה כזו באופן יחיד.
לכן קיבלנו התאמה חח"ע ועל בין $Aut(\mathbb{Z}/(n))$ לבין U_n.
נראה כי התאמה זו היא הומומורפיזם.
נניח $\varphi,\psi\in Aut(\mathbb{Z}/n)$, ונסמן $\varphi(1)=k,\ \psi(1)=r$. אזי:

$$(\psi\circ\varphi)(1)=\psi(\varphi(1))=\psi(k)=k\cdot\psi(1)=k\cdot r$$

■

למה 3.54 יהי $\alpha\in\mathbb{C}$ שורש יחידה. אזי $\mathbb{Q}(\alpha)\geq\mathbb{Q}$ הרחבת גלואה, וכן $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ אבלית.

הוכחה: יהא $n\in\mathbb{N}$ המינימלי כך ש־$\alpha^n=1$. אזי α שורש יחידה n־פרימיטיבי, ו־$\mathbb{Q}(\alpha)$ שדה הפיצול של x^n-1. לפולינום זה אין שורשים כפולים, ולכן $\mathbb{Q}(\alpha)\geq\mathbb{Q}$ הרחבת גלואה[14].
נסמן $C=\langle\alpha\rangle$ החבורה הכפלית הציקלית הנוצרת ע"י α ־ זהו שורש יחידה n־פרימיטיבי, ולכן מלמה קודמת $|C|=n$.
כל איבר ב־$Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ משרה אוטומורפיזם של C, ומקבלים איזומורפיזם בין $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ לתת חבורה של $U_n=Aut(C)$. נשים לב כי $|U_n|=n$, ולכן נקבל שיוויון, ולכן בפרט $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ אבלית. ■

[14] כי ראינו הרחבת גלואה $\Leftrightarrow$ שדה פיצול של פולינום ספרבילי

משפט גאוס

משפט 3.55 $\phi_n(x)$ אי פריק לכל n.

מסקנה 3.56 $|\mathbb{Q}_n : \mathbb{Q}| = \varphi(n)$

הוכחה: $\mathbb{Q}_n = \mathbb{Q}(\alpha_n)$, כאשר $\alpha_n = e^{\frac{2\pi i}{n}}$, ולכן:

$$|\mathbb{Q}_n : \mathbb{Q}| = deg(min\alpha_n) = \phi_n = \varphi(n)$$

■

כעת, נוכיח את משפט גאוס: **הוכחה:** נניח בשלילה כי $\phi_n(x)$ פריק. מהלמה של גאוס נובע כי יש $f, g \in \mathbb{Z}[x]$ כך ש־$f \cdot g = \phi_n(x)$, כאשר $deg(f), deg(g) \geq 1$.
לכל α, β שורשים של ϕ_n יש k כך ש־$\alpha^k = \beta$. נבחר k מינימלי כך שקיימים α, β המקיימים $f(\alpha) = g(\beta) = 0$, $\alpha^k = \beta$. ברור כי $(k, n) = 1$, מההגדרה.

הערה 3.57 כל שורש של ϕ_n הוא שורש של f או שורש של g, אך לא של שניהם, כי אין שורשים כפולים.

טענה 3.58 k ראשוני.

הוכחה: נניח בשלילה כי k אינו ראשוני. אזי, קיימים m, l כך ש־$k = m \cdot l$ (כמובן שאף מהם אינו 1). אזי:

$$(\alpha^m)^l = \alpha^k = \beta$$

אזי α^m הוא שורש של g או שורש של f, ובכל אופן נקבל סתירה למינימליות k, שהרי $m < k$.
הוכחה אלטרנטיבית - $(k, n) = 1$, ולכן אם k אינו ראשוני קיימים k, l כנ"ל. אזי גם $(l, n) = 1,\ (m, n) = 1$. לכן α^m גם הוא שורש יחידה n פרימיטיבי, ולכן שורש של ϕ_n - בסתירה למינימליות k. ■

נסמן $k = p$.
α שורש של $f(x)$, וכן α^p שורש של $g(x)$, ולכן $g(\alpha^p) = 0$. לכן α הוא שורש של $g(x^p)$ ושל $f(x)$ ובפרט הם אינם זרים. מלמה קודמת, $g, f, \phi_n \ni \mathbb{Z}[x]$, ולכן אפשר להסתכל עליהם מודולו p, כלומר, להטיל אותם לחוג F_p. נסמן את תמונתם ב־$\overline{g},\ \overline{f},\ \overline{\phi}_n$. גם שם $\overline{g} \cdot \overline{f} = \overline{\phi}_n$. אולם:

$$\overline{g}(x^p) = (\overline{g}(x))^p$$

כאשר השיוויון נובע מהמשפט הקטן של פרמה.
ראינו כי $f(x), g(x^p)$ אינם זרים (שכן יש להם שורש משותף), ולכן גם $\overline{f}(x),\ \overline{g}(x^p)$ אינם זרים, ולכן, מהשיוויון מעלה, גם $\overline{f}(x),\ \overline{g}(x)$ אינם זרים, ולכן ישנו פולינום $\psi(x) = gcd(\overline{f}, \overline{g})$ לא סקלרי ב־$F_p[x]$. אזי:

$$\psi^2 | \overline{f} \cdot \overline{g} = \overline{\phi}_n | x^n - 1$$

בחוג $F_p[x]$ - אבל קיבלנו סתירה, כי ל־$x^n - 1$ אין שורשים כפולים בשום הרחבה (מניתוח הנגזרת של פולינום זה), ולכן ϕ_n אכן אי פריק, כנדרש. ■

3/5/2011

למה 3.59 יהיו n,m זרים. אזי $U_{nm}\simeq U_n\times U_m$, ובפרט $\varphi(nm)=\varphi(n)\cdot\varphi(m)$.

הוכחה: יש הומומורפיזם טבעי בין החוגים:

$$\mathbb{Z}/(mn)\to\mathbb{Z}/(m)\times\mathbb{Z}/(n)$$

הנתון ע"י:

$$k+nm\mathbb{Z}\to(k+n\mathbb{Z},k+m\mathbb{Z})$$

העתקה זו היא על ממשפט השאריות הסיני:
"לכל $a,b\in\mathbb{Z}$, $(m,n)=1$, קיים $k\in\mathbb{Z}$ כך ש: $k\equiv a\,(modn)\equiv b\,(modm)$".
משיקולי עוצמות, ההומומורפיזם הנ"ל הוא גם חח"ע, כלומר איזומורפיזם. האיזומורפיזם הזה משרה איזומורפיזם בין חבורות ההפיכים:

$$U_{nm}\simeq U_n\times U_m$$

■

למה 3.60 באופן כללי, אם $lcm(m,n)=L,\ gcd(m,n)=d$, אזי:

$$\varphi(n)\cdot\varphi(m)=\varphi(L)\cdot\varphi(d)$$

הוכחה: נסמן $m=\prod_S p_i^{m_i},\ n=\prod_S p_i^{n_i}$, כאשר $m_i,n_i\geq 0$ שלמים, S קבוצה סופית של ראשוניים. אזי:

$$d=gcd(m,n)=\prod_S p_i^{min\{n_i,m_i\}},\ l=lcm(m,n)=\prod_S p_i^{max\{n_i,m_i\}}$$

מהלמה הקודמת:

$$\varphi(n)=\prod_S\varphi(p_i^{n_i}),\ \varphi(m)=\prod_S p_i^{m_i}$$
$$\Rightarrow\varphi(d)=\prod_S\varphi\left(p_i^{min\{n_i,m_i\}}\right),\ \varphi(l)=\prod_S\varphi\left(p_i^{max\{n_i,m_i\}}\right)$$

ומכיוון ו־$n_i+m_i=min\{m_i,n_i\}+max\{n_i,m_i\}$, נקבל:

$$\varphi(n)\cdot\varphi(m)=\varphi(L)\cdot\varphi(d)$$

■

תרגיל: חשב את $\varphi(p^n)$.

טענה 3.61 יהיו $n,m\in\mathbb{N}$, ונסמן $d=gcd(m,n)$, $L=lcm(n,m)$. אזי:

1. $\langle\mathbb{Q}_n,\mathbb{Q}_m\rangle$ - השדה המינימלי המכיל את $\mathbb{Q}_n,\mathbb{Q}_m$ הוא $\mathbb{Q}_L$.

2. $\mathbb{Q}_d = \mathbb{Q}_n \cap \mathbb{Q}_m$.

הערה 3.62 באופן כללי, אם $r|t$, אז $\mathbb{Q}_t \supseteq \mathbb{Q}_r$.
זאת מכיוון ואם $t = r \cdot s$, ו־α שורש יחידה t־פרימיטיבי, אז α^s שורש יחידה r פרימיטיבי, ואז, מההגדרה:

$$\mathbb{Q}_t = \mathbb{Q}[\alpha] \geq \mathbb{Q}[\alpha^s] = \mathbb{Q}_r$$

הוכחה:

1. מההערה, $\mathbb{Q}_n, \mathbb{Q}_m \subseteq \mathbb{Q}_L$, לכן $\langle \mathbb{Q}_n, \mathbb{Q}_m \rangle \subseteq \mathbb{Q}_L$. נראה את ההכלה בכיוון השני:
יהא α שורש יחידה n פרימיטיבי ב־$\mathbb{Q}_n$, β שורש יחידה m פרימיטיבי ב־$\mathbb{Q}_m$, ויהא γ שורש יחידה L פרימיטיבי ב־$\mathbb{Q}_L$.
$\langle \alpha, \beta \rangle \subseteq \langle \mathbb{Q}_n, \mathbb{Q}_m \rangle$, אבל $\langle \gamma \rangle \geq \langle \alpha, \beta \rangle$, ולכן $\langle \alpha, \beta \rangle$ ציקלית מסדר המתחלק ב־n, m, ולכן $\langle \alpha, \beta \rangle = \langle \gamma \rangle$. לכן $\langle \mathbb{Q}_n, \mathbb{Q}_m \rangle \subseteq \langle \alpha, \beta \rangle = \langle \gamma \rangle$.
מהכלה דו כיוונית, סיימנו.

2. **תזכורת: משפט:** יהיו $F \leq E \leq K$ שדות, כאשר E הרחבת גלואה, ויש $F \leq L \leq K$ כך ש־$K = \langle L, E \rangle$. אזי E/L הרחבת גלואה, וכן

$$|K : L| = |E : L \cap E|$$

נשתמש במשפט - אנו יודעים כי $\mathbb{Q}_n \geq \mathbb{Q}$ גלואה, $\mathbb{Q}_L = \langle \mathbb{Q}_n, \mathbb{Q}_m \rangle$ מהסעיף הקודם. לכן:

$$\frac{\varphi(L)}{\varphi(n)} = |\mathbb{Q}_L : \mathbb{Q}_n| \overset{theorem}{=} |\mathbb{Q}_m : \mathbb{Q}_n \cap \mathbb{Q}_m| \overset{remark}{\geq} |\mathbb{Q}_m : \mathbb{Q}_d| = \frac{\varphi(m)}{\varphi(d)}$$

אבל, מהלמה הקודמת, שני האגפים החיצוניים שווים, שהרי:

$$\varphi(n) \cdot \varphi(m) = \varphi(L) \cdot \varphi(d) \Rightarrow \frac{\varphi(L)}{\varphi(n)} = \frac{\varphi(m)}{\varphi(d)}$$

ולכן קיבלנו שיוויונות לאורך הביטוי, כלומר $\mathbb{Q}_d = \mathbb{Q}_n \cap \mathbb{Q}_m$.

■

16/5/2011

משפט 3.63 תהא G חבורה אבלית סופית. אזי, ישנה הרחבת גלואה $E \geq \mathbb{Q}$ כך ש:

$$G \simeq Gal(E/\mathbb{Q})$$

הערה 3.64 למעשה, נראה כי יש E כנ"ל שהוא שדה ביניים בין $\mathbb{Q}$ לאיזה הרחבה ציקלוטומית $\mathbb{Q}_n$.

את המשפט נוכיח בעזרת משפטים שראינו בעבר, וכן בעזרת משפט דיריכלה, אותו נוכיח בתרגול. המשפטים בהם נשתמש:

1. $\mathbb{Q}_n = \mathbb{Q}\left[e^{\frac{2\pi i}{n}}\right]$.

2. $|\mathbb{Q}_n : \mathbb{Q}| = deg\phi_n = \varphi(n)$, כאשר ϕ_n הוא הפולינום הציקלוטומי:

$$\phi_n = \prod_{\substack{1\leq k<n \\ (k,n)=1}} \left(x - e^{\frac{2\pi ik}{n}}\right)$$

3. $\mathbb{Q}_n \geq \mathbb{Q}$ הרחבת גלואה, וכן חישבנו את חבורת גלואה:

$$Gal\left(\mathbb{Q}_n/\mathbb{Q}\right) = U_n = \left(\mathbb{Z}/(n)\right)*$$

ובפרט היא חבורה אבלית.

4. אם n, m זרים, אזי:

$$U_{n\times m} = U_n \times U_m$$

וכן אם p ראשוני, אזי:

$$U_p \simeq \mathbb{Z}/(p-1)$$

5. משפט דיריכלה: לכל $n \in \mathbb{N}$ יש אינסוף ראשוניים מהצורה $p \equiv 1\,(modn)$.

6. ראינו מזמן (החלק השלישי של המשפט הבסיסי של חבורת גלואה) כי אם $E \geq F$ הרחבת גלואה, וכן אם $G = Gal\left(E/F\right)$, $N \triangleleft G$, $K = Fix\left(N\right)$, אזי $K \geq F$ הרחבת גלואה, וכן:

$$Gal\left(K/F\right) \simeq G/N$$

7. משפט ממבנים 1: כל חבורה אבלית סופית היא מכפלה ישרה של חבורות ציקליות.

כעת, בעזרת הנ"ל, נוכיח את המשפט: **הוכחה:** תהא G חבורה אבלית סופית. אזי, לפי 7, קיימות חבורות ציקליות C_{n_i} (מסדר n_i) כך ש:

$$G \simeq C_{n_1} \times C_{n_2} \times ... \times C_{n_k}$$

לפי 5, ישנם אינסוף ראשוניים שונים p_i כך ש־$p_i \equiv 1\,(modn_i)$. נגדיר: $r = \prod_{i=1}^{k} p_i$, ונביט בהרחבה הציקלוטומית $\mathbb{Q}_r > \mathbb{Q}$. אזי, מ־3 ו־4 היא גלואה, וכמו כן:

$$Gal\left(\mathbb{Q}_r/\mathbb{Q}\right) = \prod_{i=1}^{k} C_{(p_i-1)}$$

הערה 3.65 אם $n|m$, אזי C_n ציקלית מסדר n איזומורפית למנה של C_m, גם היא ציקלית מסדר n.

מכיוון ו־$n_i|p_i-1$ מההגדרה שלו, יש ל־C_{p_i-1} מנה איזומורפית ל־C_{n_i} (מההערה), ולכן ל־$H=\prod_{i=1}^{k}C_{p_i-1}$ יש מנה איזומורפית ל־$G\simeq\prod_{i=1}^{k}C_{n_i}$.

כלומר, ל־H יש תת חבורה נורמלית $N\triangleleft H$ כך ש־$G\simeq {}^{H}\!/_{N}$. נגדיר $E=Fix\left(N\right)$. לכן מ־6, $E\geq\mathbb{Q}$ הרחבת גלואה, וכן:

$$Gal\left({}^{E}\!/_{\mathbb{Q}}\right)\simeq {}^{H}\!/_{N}\simeq G$$

■

3.5 תורת גלואה ושדות סופיים

הערה 3.66 כאן אני משלבת טענות מתרגול וטענות שהובאו בשיעור שהעדרו של צחיק.

4 בניות בעזרת סרגל ומחוגה

בהנתן מישור, תהינו אילו בעיות נוכל לפתור בעזרת סרגל ומחוגה.
הפעולות המותרות:

- לבנות את הישר בין 2 נקודות נתונות.
- לבנות את המעגל שמרכזו a ועובר דרך b.
- בהנתן שני ישרים (לא מקבילים), אפשר לקבל את נקודת החיתוך שלהם.
- בהנתן ישר ומעגל, אפשר לקבל את נקודות החיתוך שלהם.
- בהנתן שני מעגלים, אפשר לקבל את נקודות החיתוך שלהם.

ראינו למשל שניתן למצוא את אמצע הקטע בין שתי נקודות.
כמו כן, ניתן להכפיל קטע פי שתיים, פי שלוש...
כשאחנו יודעים להכפיל - אנו יודעים גם לחלק:
נעביר מעגל ברדיוס 3 בשתי נקודות הקצה, במפגש בין שני המעגלים נעביר מעגל ברדיוס אחד, ומדמיון משולשים הבסיס של המשלוש הקטן שיותר הוא שליש.
בצורה יותר פורמלית:
בהנתן קונפיגורציה של נקודות במישור, אפשר להעביר ישרים בין נקודות נתונות, עיגול סביב נקודה במרחק שידוע (כלומר מרחק בין נקודות מקבוצה שיש), ולקבל חיתוכים. ראינו:

הגדרה 4.1 $E_{\mathbb{R}}$ קבוצת כל הנקודות על ציר x הניתנות לבניה, כאשר הקבוצה ההתחלתית היא $(0,0),(1,1)$.

טענה 4.2

1. $E_{\mathbb{R}}$ שדה המכיל את $\mathbb{Q}$.
2. $(x,y)\subseteq\mathbb{R}^2$ ניתנת לבניה אמ"מ $x,y\in E_{\mathbb{R}}$.

טענה 4.3 אם $E_{\mathbb{R}}\ni x>0$, אז $E_{\mathbb{R}}\ni\sqrt{x}$.

הוכחה: בציור! יסרק בהמשך. ■

טענה 4.4 בהנתן נקודות $p_1,...,p_n$ כך ש-$p_i=(x_i,y_i)$, אזי $E:=E(p_1,...,p_n)$ הוא השדה המינימלי המכיל את x_i,y_i לכל $i=1,...,n$ ואת המרחקים $\|p_i-p_j\|$, ואם p ניתן לבניה בצעד אחד מ-$\{p_1,...,p_n\}$, כלומר, אם p הוא חיתוך של ישר עם מעגל עם ישר או מעגל המוגדרים מ-$\{p_1,...,p_n,\}$אזי, אם $p=(x,y)$, או $x,y\in E$, או ש-$x,y\in E(\sqrt{\alpha})$ לאיזה $\alpha\in E$.

הוכחה: אפילו בספר לא מופיעה, צריך לבדוק, "לא יודע אם יש לו כוח לעשות אותה... זה לא כל כך ארוך, אני פשוט מתעצל". נראה אם אצליח למצוא אותה\לסדר את מה שצחיק אמר בעל פה בהמשך. ■

כמסקנה מהמשפט, נביא משפט:

משפט 4.5 $E_{\mathbb{R}}$ הוא השדה המינימלי שמכיל את $\mathbb{Q}$ וסגור ללקיחת שורשים של חיוביים.

טענה 4.6 $E_{\mathbb{C}} = E_{\mathbb{R}} + iE_{\mathbb{R}}$, כלומר $E_{\mathbb{C}} = \{x+iy | x,y \in E_{\mathbb{R}}\}$.

מסקנה 4.7 $E_{\mathbb{C}}$ שדה.

הערה 4.8 אם $x+iy \in E_{\mathbb{C}}$, אזי $x^2+y^2 \in E_{\mathbb{R}}$.

טענה 4.9 $E_{\mathbb{C}}$ סגור ללקיחת שורשים.

הוכחה: להוציא שורש למספר מרוכב בהצגה פולרית הוא הוצאת שורש לרדיוס וחציית זווית - ואלו דברים שניתן לעשות בעזרת מחוגה וסרגל (ציור, יסרק בתקווה בהמשך):
ניקח מעגל ברדיוס a מהנקודה $x+iy$, ומעגל נוסף ברדיוס זה מהנקודה (c,d) (הציור ההגדרה של הנקודה הזו...?). בחיתוך של שני המעגלים נמתח ישר ל-$(0,0)$- ישר זה יחצה לנו את הזווית. ■

משפט 4.10 $E_{\mathbb{C}}$ הוא השדה המינימלי ב-$\mathbb{C}$ המכיל את $\mathbb{Q}$ וסגור ללקיחת שורשים.

הוכחנו זאת כבר המשפט האנלוגי ל-$E_{\mathbb{R}}$.

מסקנה 4.11 אם $\alpha \in \mathbb{C}$ ניתן לבניה, אזי α אלגברי מעל $\mathbb{Q}$, וכן $|\mathbb{Q}[\alpha] : \mathbb{Q}|$ = חזקה של 2.

הוכחה: אם α ניתן לבניה, אז יש סדרה סופית של הרחבות:

$$\mathbb{Q} \leq E_0 \leq E_1 \leq ... \leq E_r$$

כך ש-E_i/E_{i-1} הוא הרחבה ריבועית לכל $i = 1, ..., r$ (מטענות קודמות - בכל פעם אנחנו מוסיפים איבר על ידי צעד של בניה בעזרת סרגל ומחוגה). לכן $E_r/\mathbb{Q}$ הוא מסדר 2^r. אבל $\mathbb{Q} \leq \mathbb{Q}[\alpha] \leq E_r$, ולכן $|\mathbb{Q}[\alpha] : \mathbb{Q}] \, | 2^r$. ■

הטענה ההפוכה אינה נכונה, אבל ניתן לאפיין בדיוק את המספרים הניתנים לבניה.

4.1 בעיות בניה מפורסמות ללא פתרון

1. "לרבע את המעגל" - או "לשטוח את המעגל" (שתי הבעיות שקולות), כלומר, בהנתן מעגל ומרכזו, לא ניתן לבנות ריבוע ששטחו שווה לשטח המעגל.

   הוכחה: נקבע יחידות כך שרדיוס המעגל הוא 1 ושטחו הוא π. הבעיה המתפרשת לשאלה זו היא האם $\sqrt{\pi}$ ניתן לבניה. אבל ידוע כי π אינו אלגברי, ובפרט איננו ניתן לבניה. ■

2. "להכפיל את הקוביה" - בהנתן קוביה, האם אפשר בעזרת מחוגה וסרגל לבנות קוביה בנפח כפול?
   בעיה זו מתפרשת לשאלה - האם ניתן לבנות את $\sqrt[3]{2}$.

   טענה 4.12 אי אפשר.

   הוכחה: $\sqrt[3]{2}$ מקיים את הפולינום $x^3 - 2$. זהו פולינום א"פ ממעלה 3, ולכן $|\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}| = 3$, כלומר איננו חזקת 2, ולכן איננו ניתן לבניה. ■

3. "לשלש זווית" - כלומר, האם ניתן לחלק זווית לשלושה חלקים שווים?

טענה 4.13 לא תמיד!

הוכחה: π נתון. את $\frac{\pi}{3}$ ניתן לבנות, אך את השליש של זווית זו - $\frac{\pi}{9}$ אי אפשר.

לו היה אפשר, אזי היה ניתן לבנות גם את $e^{\frac{2\pi i}{18}}$, אבל: $\mathbb{Q}\left[e^{\frac{2\pi i}{18}}\right] = \mathbb{Q}_{18}$ הרחבה ציקלוטומית, ולכן מסדר $\varphi(18) = 6$, וזה איננו חזקה של 6 - דהיינו, מספר זה איננו ניתן לבניה. ■

היוונים, מלבד בעיות אלו, לא הצליחו לבנות מצולע משוכלל עם 17 צלעות. גאוס הצליח, ומספרים שכל כך התלהב מההוכחה שלו, שהחליט להיות מתמטיקאי ולא בלשן.

בהוכחה זו, גאוס התבסס על וריאציה של הטענה ההפוכה מהמסקנה שהבאנו קודם:

4.2 תורת גלואה ובניות בעזרת סרגל ומחוגה

משפט 4.14 $\alpha \in \mathbb{C}$ ניתן לבניה אמ"מ α שייך לאיזה שדה E כך ש-$|E:\mathbb{Q}| = 2^n$ לאיזה n, וכן $E \geq \mathbb{Q}$ הרחבת גלואה.

17/5/2011

הערה 4.15 הרחבה מסדר 2 היא תמיד נורמלית, כי אם $|E:F| = 2$, אזי $E = F(\beta)$ עבור איזה β המקיים פולינום מסדר 2- פולינום זה מתפצל מעל E, כי עבור פולינום ממעלה 2, אם שורש אחד ב-E, אזי גם השורש השני ב-E:

$$\frac{p(x)}{(x-\beta)} = a(x-\alpha)$$

ואז α גם בשדה הזה, ולכן הפולינום יתפצל מעל E, ולכן E נורמלית.

תרגיל: אם $E \geq K$ ו-$K \geq F$ נורמלית, אזי $E \geq F$ לא בהכרח נורמליות - מצאו דוגמא לכך.

הערה 4.16 אם $E \geq F$ נורמלית, ו-K שדה ביניים - $E \geq K \geq F$, אזי $E \geq K$ נורמלית.

הוכחה: יהי $L \geq E$, ויהי $\sigma \in Gal(L/K)$. אזי $\sigma \in Gal(L/F)$, ולכן $\sigma(E) = E$, כי $E \geq F$ נורמלית. ■

23/5/2011

נוכיח את המשפט: **הוכחה:** $\Leftarrow$ נניח כי α ניתן לבניה. אזי ראינו כי ישנה סדרת הרחבות (סופית):

$$\mathbb{Q} = F_0 \leq F_1 \leq ... \leq F_k$$

כך ש-$|F_i : F_{i-1}| = 2$ לכל $i = 1, ..., k$, $\alpha \in F_k$. נשים לב כי אין טרנזיטיביות להיות הרחבה הרחבת גלואה - כלומר, אם $F_i \geq F_{i-1}$ גלואה, אין זה אומר כי $F_i \geq F_{i-2}$ גלואה, וכו'.

נראה באינדוקציה על $k \in \mathbb{N}$ שיש $F_k \leq E$ כך ש-$|E:\mathbb{Q}|$ חזקת 2, וכן כי $E \geq \mathbb{Q}$ נורמלית.

בסיס: עבור $k = 0$ - ברור, ניקח $E = F_0$.

הנחה: נניח כי יש $E_0 \geq F_{k-1}$ כך ש־$|E_0 : \mathbb{Q}|$ = חזקת 2, וכן $E_0 \geq \mathbb{Q}$ גלואה.
צעד: נסמן $F_k = F_{k-1}(\alpha)$, ונניח $\alpha \notin F_{k-1}$ (אם היה, אז מהנחת האינדוקציה הוא ניתן לבניה, וסיימנו). α מקיים פולינום ריבועי מעל F_{k-1}, לכן הוא מקיים פולינום ממעלה ≥ 2 מעל E_0 (כי הוא מכיל את F_{k-1}). אם $\alpha \in E_0$ סיימנו. אחרת, α מקיים פולינום $f \ni E_0[x]$ ממעלה 2.
נגדיר $g(x) = \prod_{\sigma \in Gal(E_0/\mathbb{Q})} \overline{\sigma}(f)$, כאשר $\overline{\sigma}$ היא הפעלת σ על מקדמי f. נטען כי $g \in \mathbb{Q}[x]$ ־ זה נכון, כי לכל $\tau \in Gal(E_0/\mathbb{Q})$:

$$\overline{\tau}(g) = \prod_{\sigma \in Gal(E_0/\mathbb{Q})} \overline{\tau}\overline{\sigma}(f) = \prod_{\sigma \in Gal(E_0/\mathbb{Q})} \overline{\sigma}(f) = g$$

$E_0/\mathbb{Q}$ גלואה, כלומר איברי $Gal(E_0/\mathbb{Q})$ הם כל האוטומורפיזמים המקבעים את איברי $\mathbb{Q}$. הם מקבעים את g, ולכן $g \in \mathbb{Q}[x]$.
יהא E' שדה פיצול של g מעל $\mathbb{Q}$. g ספרבילי, כי הוא פולינום מעל שדה עם מציין 0, ולכן ממשפט קודם $E' \geq \mathbb{Q}$ גלואה. נגדיר $E = \langle E', E_0 \rangle$. מכיוון ו־$E', E_0$ גלואה, גם $E \geq \mathbb{Q}$ גלואה.

הערה 4.17 עובדה שכדאי לדעת ־ במציין אפס, להיות גלואה $\Leftrightarrow$ ספרבילי ונורמלי $\Leftrightarrow$ כל אוטומורפיזם של $\mathbb{C}$ שומר על השדה $\Leftrightarrow$ כל אוטומורפיזם של $\mathbb{C}$ יקח את E', E_0 לעצמם.

נותר רק להראות כי $|E : \mathbb{Q}|$ = חזקת 2.
E הוא שדה פיצול של g מעל E_0 (כי הוא מכיל את E_0 ואת E' ־ המכיל את כל השורשים של g, וכן הוא השדה המינימלי המכיל את שניהם). אבל, כל שורש של g הוא למעשה שורש של $\overline{\sigma}(f)$ לאיזה $\sigma \in Gal(E_0/\mathbb{Q})$, ולכן מקיים פולינום ממעלה 2 מעל E_0. לכן $|E : E_0|$ = חזקת 2, ולכן גם:

$$|E : \mathbb{Q}| = |E : E_0| \cdot |E_0 : \mathbb{Q}|$$

הוא חזקת 2.
$\Rightarrow$ נניח כי $E \geq \mathbb{Q}$, $\alpha \in E$ הרחבת גלואה מסדר 2^n. נוכיח באינדוקציה על n כי אם $E \geq F$ גלואה מסדר 2^n, אזי יש סדרה:

$$F = F_0 \leq F_1 \leq ... \leq F_n = E$$

כך ש־$|F_i : F_{i-1}| = 2$.
בסיס: עבור $n = 0$ ־ $\alpha \in \mathbb{Q}$, וההנחה ברורה.
צעד: כאמור, אנו מניחים כי:

$$G = Gal(E/\mathbb{Q}),\ |E : \mathbb{Q}| = 2^n$$

לכן, ל־G יש מרכז לא טריוויאלי (ממשפט שראינו במבנים 1 כי החבורה היא מחזקת ראשוני, כלומר p סילוא), ובפרט יש תת חבורה $Z \triangleleft G$ לא טריוויאלית.
נגדיר $K = Fix(Z)$. אזי $K \geq \mathbb{Q}$, וכן $E \geq K$ גלואה, ולכן $|K : \mathbb{Q}|\,|2^n,\ |E : K|\,|2^n$, כלומר $|K : \mathbb{Q}| = 2^l,\ |E : K| = 2^m$ עבור $l, m < n$. מהנחת האינדוקציה, יש סדרות:

$$F = F_0 \leq F_1 \leq ... \leq F_l = K,\ K = F_l \leq F_{l+1} \leq \underbrace{F_{l+m}}_{=n} = E$$

כך ש־$|F_i : F_{i-1}| = 2$, וסיימנו! ■

זהו משפט שימושי להראות שמספרים מסויימים ניתנים לבניה, מספרים שהיוונים לא הצליחו להראות קיום בניה "בכוח".

5 שורשים ורדיקלים מעל $\mathbb{Q}$

5.1 הגדרות

17/5/2011

אנו מכירים מהתיכון כי הפתרונות למשוואה ריבועית $ax^2+bx+c=0$ ניתנים על ידי הנוסחא:

$$X_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

הרבה יותר קשה לפתור משוואה ממעלה 3 ומעלה , אבל זה אפשרי - קיימות נוסחאות המשתמשות ב־4 פעולות החשבון והוצאת שורשים אשר בעזרתן ניתן למצוא את הפתרון.

הגדרה 5.1 פתרון משוואה בעזרת 4 פעולות חשבון והוצאת שורשים נקרא פתרון ברדיקלים.

נשאלת השאלה - האם לכל משוואה קיים פתרון ברדיקלים?

הגדרה 5.2 הרחבת שדות $E\geq F$ נקראת הרחבה רדיקלית, אם $E=F(\alpha)$ עבור α המקיים $\alpha^n\in F$ לאיזה n. כלומר, עבור $a\in F$ כלשהוא, $\alpha=\sqrt[n]{a}$.

הגדרה 5.3 הרחבה רדיקלית נשנית (repeated) היא הרחבה $E\geq F$ עבורה יש סדרה סופית:

$$F=E_0\leq E_1\leq ...\leq E_n=E$$

כך ש־$E_i\geq E_{i-1}$ רדיקלית.

הגדרה 5.4 פולינום $p(x)\in\mathbb{Q}[x]$ נקרא פתיר ברדיקלים אם $p(x)$ מתפצל באיזה הרחבה רדיקלית נשנית.

הערה 5.5 כלומר, שדה הפיצול שלו מוכל בהרחבה רדיקלית נשנית - אין זה אומר ששדה הפיצול עצמו הוא הרחבה רדיקלית נשנית.

סימון: עבור $p\in\mathbb{Q}[x]$, נגדיר $Gal(p)=Gal(E/\mathbb{Q})$ כאשר E הוא שדה הפיצול של p ב־$\mathbb{C}$.

למה 5.6 תהי $E\geq F$ הרחבה, $E\geq K,L\geq F$ שדות ביניים כך ש־$K\geq F,\ L\geq F$ הן הרחבות רדיקליות נשנות (הר"נ). אזי גם $\langle K,L\rangle$ הר"נ.

הוכחה: נתון כי $K\geq F,\ L\geq F$ הן הר"נ, לכן קיימות סדרה:

$$F\leq F[\alpha_1]\leq F[\alpha_1,\alpha_2]\leq ...\leq F[\alpha_1,...,\alpha_m]=K$$

עבור $\alpha_1,...,\alpha_m\in E$, כך ש־$\alpha_i^{n_i}\in F[\alpha_1,...,\alpha_{i-1}]$ לכל $i\leq n$ לאיזה $n_i\in\mathbb{N}$ (כלומר, הן כולן הרחבות רדיקליות). באופן דומה, קיימת גם סדרה:

$$F\leq F[\beta_1]\leq F[\beta_1,\beta_2]\leq ...\leq F[\beta_1,...,\beta_r]=L$$

כך ש־$\beta_i^{l_i}\in F[\beta_1,...,\beta_{i-1}]$ לכל $i\leq r$ לאיזה $l_i\in\mathbb{N}$.

$\langle K,L\rangle = F[\alpha_1,...,\alpha_m,\beta_1,...,\beta_r]$, לכן, אם נשלב את הסדרות מעלה, נקבל:

$$F \leq F[\alpha_1] \leq ... \leq F[\alpha_1,...,\alpha_m] \leq F[\alpha_1,...,\alpha_m,\beta_1] \leq ... \leq F[\alpha_1,...,\alpha_m,\beta_1,...,\beta_r] = \langle K,L\rangle$$

כאשר כל ההרחבות הללו רדיקליות, ולכן גם $\langle K,L\rangle$ הר"נ, כנדרש. ■

מסקנה 5.7 אם $E \geq F$ הרחבה כלשהיא, אזי:

1. איחוד של שדות הביניים שהם הר"נ של F הוא שדה.
2. אם $|E:F| < \infty$ אזי האיחוד הנ"ל הוא בעצמו הר"נ.

הוכחה: :

1. יהא K איחוד כל שדות הביניים שהם הר"נ של F. אם $\alpha,\beta \in K$, צ"ל כי $K \supseteq F(\alpha,\beta)$. יהי $L \geq F(\alpha)$ שהוא הר"נ של F, וכן $R \geq F(\beta)$ שהוא הר"נ של F, ולכן $\langle L,R\rangle \supseteq F(\alpha,\beta)$, שלפי הלמה קודמת הוא גם הר"נ - ולכן מוכל ב-K.
2. נניח $|E:F| < \infty$, ויהא $F \leq K \leq E$ הר"נ של F כך ש-$|K:F|$ מקסימלי. אם $F \leq L \leq E$ שדה ביניים שהוא הר"נ של F, אזי $L \subseteq K$. אחרת, $\langle L,K\rangle$ הר"נ גדול יותר, בסתירה להנחת המקסימליות של K.

■

למה 5.8 פולינום אי פריק $p \in \mathbb{Q}[x]$ הוא פתיר ברדיקלים אמ"מ יש לו שורש באיזה הר"נ.

הוכחה: צד אחד טריוויאלי מההגדרה - כי פתיר ברדיקלים משמע שהוא מתפצל באיזה הר"נ - אם הוא מתפצל באיזה הר"נ, אזי יש לו שורש שם.

מצד שני, נניח כי α שורש של p כך ש-$\alpha \in E \geq \mathbb{Q}$, E הרחבה רדיקלית נשנית, ויהא L שדה הפיצול של p מעל $\mathbb{Q}$ - כלומר L הרחבת פיצול של פולינום ספרבילי (כי כל פולינום הוא ספרבילי ב-$\mathbb{Q}$), ולכן זוהי הרחבת גלואה של $\mathbb{Q}$.

יהא $K \subseteq \langle E,L\rangle$ כלשהוא כך ש-$K \geq \mathbb{Q}$ הרחבת גלואה. שורשי p הם איברי הקבוצה $\{\sigma(\alpha)\,|\sigma \in Gal(K/\mathbb{Q})\}$.

$\sigma(\alpha) \in \sigma(E) \subseteq K$, וכן $\mathbb{Q} \leq \sigma(E)$ הר"נ, כי:

$$\mathbb{Q} \subseteq \mathbb{Q}[\beta_1] \subseteq \mathbb{Q}[\beta_1,\beta_2] \subseteq ... \subseteq \mathbb{Q}[\beta_1,...,\beta_m] = E$$

כך ש-$\beta_i^{n_i} \in \mathbb{Q}[\beta_1,..,\beta_{i-1}]$. לכן:

$$\mathbb{Q} \subseteq \mathbb{Q}[\sigma(\beta_1)] \subseteq ... \subseteq \mathbb{Q}[\sigma(\beta_1),...,\sigma(\beta_m)] = \sigma(E)$$

כך ש-$\sigma(\beta_i^{n_i}) \in \mathbb{Q}[\sigma(\beta_1),..,\sigma(\beta_{i-1})]$.

יהא $\mathbb{Q} \leq R \leq K$ הר"נ המקסימלי. אזי $\sigma(\alpha) \subseteq R$ לכל $\sigma \in Gal(K/\mathbb{Q})$, ולכן p מתפצל מעל R. ■

5.2 פיתוח הכלים והוכחת משפט גלואה

משפט גלואה

משפט 5.9 $p \in \mathbb{Q}[x]$ (או בכל שדה ממציין 0 אחר) פתיר ברדיקלים אמ"מ $Gal(p)$ פתירה.

דוגמא:
$f(x) = 2x^5 - 10x + 5$ מקיים $Gal(f) = Sym(5)$. זוהי חבורה שאינה פתירה, ועל כן, ממשפט גלואה, f איננו פתיר ברדיקלים. 23/5/2011
נוכיח אותו בהמשך. לפני כן, נפתח כלים שיעזרו לנו בהוכחה.

5.2.1 הלמה של דדקינד ווריאציה שלה

למה 5.10 יהא E שדה. אזי אברי $Aut(E)$ הם בת"ל במרחב הפונקציות מ־E ל־E (כמ"ו מעל E).

הוכחה: נניח בשלילה כי הטענה אינה נכונה. יהא $n \in \mathbb{N}$ מינימלי כך ש־$\sigma_1, ..., \sigma_n \in Aut(E)$ שונים, וכן $a_1, ..., a_n \in E$ כך ש־$\sum_{i=1}^{n} a_i \sigma_i = 0$, ובפרט כל $a_i \neq 0$ לכל i.

$\sigma_1 \neq \sigma_2$, לכן יש איבר $b \in E$ כך ש־$\sigma_1(b) \neq \sigma_2(b)$. נשים לב כי $\sum_{i=1}^{n} a_i \sigma_i(b\gamma) = 0$ לכל $\gamma \in E$, אבל:

$$0 = \sum_{i=1}^{n} a_i \sigma_i(b\gamma) = \sum_{i=1}^{n} a_i \sigma_i(b)\,\sigma_i(\gamma)$$
$$\Rightarrow 0 = \sum_{i=1}^{n} (a_i \sigma_i(b))\,\sigma_i$$

נסמן שיוויון זה ב־$(**)$. מצד שני,

$$\sum_{i=1}^{n} a_i \sigma_i = 0 \Rightarrow 0 = \sigma_1(b) \cdot 0 = \sigma_1(b) \cdot \sum_{i=1}^{n} a_i \sigma_i = \sum_{i=1}^{n} (a_i \sigma_1(b))\,\sigma_i$$

נסמן משוואה זו ב־$(***)$. נחסר את $(**)$ מ־$(***)$, ונקבל:

$$0 = \sum_{i=1}^{n} [a_i(\sigma_i(b) - \sigma_1(b))]\,\sigma_i = \sum_{i=2}^{n} [a_i(\sigma_i(b) - \sigma_1(b))]\,\sigma_i$$

והמקדם $a_2(\sigma_2(b) - \sigma_1(b)) \neq 0$, וקיבלנו תלות קצרה יותר, בסתירה להנחה! ■

אנחנו נשתמש בוריאצה של הלמה הזו:

למה 5.11 יהא $G \leq Aut(E)$ סופית, $F = Fix(G)$, ויהא $\theta : G \to F*$ הומומורפיזם.
אזי יש $\alpha \in E*$ עבורו $\theta(\tau) = \frac{\tau(\alpha)}{\alpha}$ לכל $\tau \in G$.

הוכחה: מהלמה של דדיקינד, $\sum_{\sigma \in G} \theta(\sigma)\,\sigma \neq 0$, כלומר יש $\gamma \in F*$ כך ש:

$$\beta := \sum_{\sigma \in G} \theta(\sigma)\,\sigma(\gamma) \neq 0$$

נגדיר $\alpha = \frac{1}{\beta}$. אזי:

$$\forall \tau \in G \tau(\beta) = \tau\left(\sum_{\sigma\in G}\theta(\sigma)\sigma(\gamma)\right) = \sum_{\sigma\in G}\tau\left(\overbrace{\theta(\sigma)}^{\in F*}\right)\cdot\tau(\sigma(\gamma)) \overset{F=Fix(G)}{=} \sum_{\sigma\in G}\theta(\sigma)\cdot(\tau\sigma)(\gamma)$$

$$\Rightarrow \theta(\tau)\tau(\beta) = \sum_{\sigma\in G}\theta(\tau)\theta(\sigma)\cdot(\tau\sigma)(\gamma) = \underbrace{\sum_{\sigma\in G}\theta(\tau\sigma)\cdot(\tau\sigma)(\gamma)}_{=\beta}$$

$$\Rightarrow \theta(\tau) = \frac{\beta}{\tau(\beta)} = \frac{\tau(\alpha)}{\alpha}$$

■

5.2.2 משפט קומר

משפט 5.12 תהי $F \leq E$ הרחבה, ונניח כי E מכיל שורש יחידה n־פרימיטיבי. אזי התנאים הבאים שקולים:

1. $E \geq F$ היא גלואה ו־$Gal(E/F)$ ציקלית מסדר המחלק את n.
2. $E = F[\alpha]$ לאיזה α המקיים $\alpha^n \in F$ (כלומר ההרחבה רדיקלית).

הוכחה: נשתמש בוריאציה מהלמה של דדקינד.
יהא $\delta \in F$ שורש יחידה n־פרימיטיבי.
$1 \Leftarrow 2$: מהנחת 1, ישנו שיכון:

$$\theta : Gal(E/F) \to \langle\delta\rangle$$

כאשר $Gal(E/F)$ הוא מסדר המחלק את n מהנתון.
אזי, מהמסקנה של הלמה של דדיקינד, ישנו $\alpha \in E$ עבורו $\theta(\tau) = \frac{\tau(\alpha)}{\alpha}$ לכל $\tau \in Gal(E/F)$.
מכיון ו־E/F גלואה, על מנת להראות כי $E = F[\alpha]$ מספיק להראות כי אם $\sigma \in Gal(E/F[\alpha])$ אזי $\sigma = id_E$.
יהא $\sigma \in Gal(E/F[\alpha])$. אזי $\sigma(\alpha) = \alpha$. בפרט $\sigma \in Gal(E/F)$, ולכן $\theta(\sigma) = \frac{\sigma(\alpha)}{\alpha} = 1$, כלומר $\sigma = id_E$.
שנית, נראה כי $\alpha^n \in F$. $\frac{\sigma(\alpha)}{\alpha} \ni \langle\delta\rangle$, לכן לכל $\sigma \in Gal(E/F)$:

$$1 = 1^n = \left(\frac{\sigma(\alpha)}{\alpha}\right)^n = \frac{\sigma(\alpha^n)}{\alpha^n}$$

לכן $\sigma(\alpha^n) = \alpha^n$, כלומר $\alpha^n \in F$ (כי σ מקבעת את איברי F ואיברים אלו בלבד כי ההרחבה היא גלואה).
$2 \Leftarrow 1$: יהי $\alpha^n = a \in F$. נביט בפולינום $p(x) = x^n - a$. שורשיו הם $E \ni \alpha \cdot \delta^i$ עבור $n \leq i \leq 1$, ולכן p מתפצל מעל E, וכן E הוא שדה הפיצול של E מעל F (כי הוא הרחבה הקטנה ביותר המכילה את כל שורשי p). p ספרבילי, ולכן $E \geq F$ גלואה כהרחבת פיצול של פולינום ספרבילי.

נשים לב כי לכל $\tau \in Gal\left(E/F\right)$, $\tau\left(\alpha\right)$ גם שורש של p, ולכן $\tau\left(\alpha\right) = \alpha \cdot \delta^i$ לאיזה i. לכן נקבל:

$$\forall 1 \leq i \leq n \ \frac{\tau\left(\alpha\right)}{\alpha} = \delta^i \in F$$

נגדיר $\theta : Gal\left(E/F\right) \to \langle\delta\rangle$ ע"י $\theta\left(\tau\right) = \frac{\tau(\alpha)}{\alpha}$. נראה שזה הומומורפיזם חח"ע:

$$\theta\left(\sigma\tau\right) = \frac{\sigma\tau\left(\alpha\right)}{\alpha} = \frac{\sigma\tau\left(\alpha\right)}{\sigma\left(\alpha\right)} \cdot \frac{\sigma\left(\alpha\right)}{\alpha} = \sigma\left(\frac{\tau\left(\alpha\right)}{\alpha}\right) \cdot \frac{\sigma\left(\alpha\right)}{\alpha} = \frac{\tau\left(\alpha\right)}{\alpha} \cdot \frac{\sigma\left(\alpha\right)}{\alpha} = \theta\left(\sigma\right) \cdot \theta\left(\tau\right)$$

יהי $\tau \neq id$. אזי $\tau\left(\alpha\right) \neq \alpha$, כי $E = F\left[\alpha\right]$, ואז:

$$\theta\left(\tau\right) = \frac{\tau\left(\alpha\right)}{\alpha} \neq 1$$

לכן θ חח"ע.

לכן $Gal\left(E/F\right)$ איזומורפית (לא על!) לתת חבורה של $\langle\delta\rangle$, ולכן היא ציקלית מסדר המחלק את n. ■

5.2.3 הוכחת משפט גלואה

למה 5.13 יהיו $F = F_0 \leq F_1 \leq ... \leq F_r = L$ כאשר $F_{i-1} \leq F_i$ גלואה אבלית. יהא $F \leq E \leq L$ כך ש־$E \geq F$ גלואה.
אזי $Gal\left(E/F\right)$ פתירה.

הוכחה: נוכיח באינדוקציה על r:
בסיס - עבור $r = 1$ - כל מנה של חבורה אבלית היא אבלית. לכן:

$$Gal\left(E/F\right) = \frac{Gal\left(L/F\right)}{Gal\left(L/E\right)}$$

אבלית.
נניח כי הטענה מתקיימת עבור $r < s$, ונוכיח עבור s.
יהיו $F = F_0 \leq F_1 \leq ... \leq F_s = L$, כאשר $F \leq E \leq L$, $F \leq E$ גלואה.
נגדיר $E* = \langle E, F_1\rangle$. אזי $F_1 \leq E* \leq L$.
$F_1 \leq F_2 \leq ... \leq F_s = L$. זוהי שרשרת באורך $s-1$, וכן $E* \leq F_s = L$, $F_1 \leq E*$ גלואה ממשפט קודם. לכן, מהנחת האינדוקציה, $Gal\left(E*/F_1\right)$ פתירה.
בנוסף, ממשפט קודם נקבל כי:

$$Gal\left(E*/F_1\right) \simeq Gal\left(E/E \cap F_1\right)$$

נבחן את ההרחבה $F_1 \geq E \cap F_1 \geq F$. מכיוון ו־$F_1 \geq F$ גלואה אבלית (מהנתון), אזי כל שדה ביניים בעצמו, ובפרט $E \cap F_1$, הוא חבורת גלואה אבלית של F (כי כל תת חבורה של חב' אבלית היא נורמלית עם מנה אבלית). לכן בפרט $E \cap F_1 \geq F$ נורמלית, וכמו כן מהמשפט היסודי של חבורת גלואה:

$$Gal\left(E \cap F_1/F\right) \simeq {Gal(E/F)}/{Gal(E/E \cap F_1)}$$

כאשר כאמור $Gal\left(E/E\cap F_1\right)$ אבלית, $Gal\left(E\cap F_1/F\right)$ פתירה (כי איזומורפית לחבורה פתירה מהנחת האינדוקציה).

אבל, אם G עם תת חבורה נורמלית פתירה H כך ש־G/H פתירה, אזי ממשפט ממבנים 1, גם G פתירה, ובפרט נקבל כי $Gal\left(E/F\right)$ פתירה, כנדרש. ■

משפט 5.14 יהי $f\in F\left[x\right]$ כאשר המציין של F הוא 0, ויהי E שדה הפיצול שלו.
אזי f פתיר ברדיקלים אמ"מ $Gal\left(E/F\right)$ פתירה.

הוכחה: בכיוון הראשון, נניח כי E/F פתירה. עלינו להראות כי f פתיר ברדיקלים, כלומר כי E מוכל בהרחבה רדיקלית נשנית.

נסמן $n=\left|E:F\right|=\left|Gal\left(E/F\right)\right|$, וכן $charF=0$, לכן קיימת הרחבה ציקלוטומית $K\geq F$, $K=F\left(\delta\right)$ עבור שורש יחידה n־פרימיטיבי (שכן 0 לא מחלק את n).

נסמן $L=\left\langle K,E\right\rangle$.

ממשפט קודם, $L\geq K$ גלואה, וכן $Gal\left(L/K\right)\simeq Gal\left(E/E\cap K\right)$, ובפרט פתירה, כי החבורה הימנית פתירה כתת חבורה של $Gal\left(E/F\right)$.

ראינו כי $K\geq F$ גלואה אבלית (כהרחבה ציקלוטומית). $G=Gal\left(E/F\right)$ פתירה, ולכן יש סדרה יורדת של תתי חבורות:

$$G=N_0\triangleright N_1\triangleright ...\triangleright N_r=\left\{1\right\}$$

כך ש־N_i נורמלית ב־N_{i-1}, והמנה N_i/N_{i+1} ציקלית (אבלית - ולכן מכפלה ישרה של ציקליות, ולכן אפשר בקלות לעדן).

נגדיר $F_i=Fix\left(N_i\right)$. נשים לב כי $\left|G\right|=n$ $\left|N_i/N_{i+1}\right|\left|\left|G\right|\right.$. נגדיר $F*=\left\langle F_i,K\right\rangle$. $F_{i+1}*/F_{i}*$ גלואה ציקלית, וקיבלנו סדרת הרחבות:

$$F\leq K\leq F_1*\leq F_2*\leq ...\leq L$$

כך ש$F\leq K$ ציקלוטומית (לאו דווקא ציקלית), ושאר הן ציקליות מסדרים המחלקים את n.

כאמור $F_{i+1}*\geq F_i*$ גלואה ציקלית מסדר המחלק את n. בנוסף $\delta\in K\subseteq F_i*$, ולכן יש ב־$F_n$ שורש יחידה n־פרימיטיבי.

לכן, ממשפט קומר, $F_{i+1}*=F_i*\left[\alpha\right]$ עבור α המקיים $\alpha^n\in F_i*$, ולכן כל ההרחבות בסדרה הנ"ל רדיקליות, ולכן E מוכל בהרחבה רדיקלית משנית.

בכיוון השני, נניח כי $F\leq E\leq L$, כאשר L הרחבה רדיקלית משנית (כלומר f פתיר ברדיקלים):

$$F=F_0\leq F_1\leq ..\leq F_r=L$$

ממשפט קומר, $F_{i+1}=F_i\left(\alpha_i\right)$ עבור $\alpha_i\in F_{i+1}$ המקיים $\alpha_i^{n_i}\in F_i$. ניקח $n=\prod_{i=1}^{r}n_i$.

יהא K כמקודם - הרחבה n־ציקלוטומית של E. שוב נגדיר $F_i*=\left\langle F_i,K\right\rangle$, $L*=\left\langle L,K\right\rangle$.

עדיין מתקיים $F_{i+1}*=F_i\left[\alpha\right]$, ועדיין $\alpha_i^{n_i}\in F_i*$. אבל בנוסף $K\subseteq F_i*$, ולכן יש ב־F_i* שורש יחידה n פרימיטיבי.

ממשפט קומר, נקבל כי $F_{i+1}*\geq F_i*$ גלואה ציקלית. ושוב נקבל סדרת הרחבות:

$$F\leq K\leq F_1*\leq ..\leq F_r*=L*$$

כאשר $F\leq K$ ציקלוטומית ולכן אבלית, ושאר ההרחבות כאמור גלואה ציקליות. ולכן מהלמה הקודמת, $Gal\left(E/F\right)$ פתירה, כנדרש! ■