

2/3/09

אלגברה ב' 2 - שיעור מס' 1

(אז: מרגל גלואה)

המורה והמרגל: דוד גינזבורג

השעה האחרונה בשבוע מוקדש למרגל. השאור - שיעור.

התרגילים יתפרסמו באתר: <http://www.math.tau.ac.il/~ginzburg>

אין חובה השעה, אין בדיוק תרגילים.

"אני מודה שאני לא פותר כל תרגיל שאני מפרסם.

אני מניח שרוב התרגילים פתורים"

אלפין ודוא"ל: ginzburg@post.tau.ac.il 6405376

משרד ושעה קבילה: שריבר 315, יום שני 11⁰⁰-10⁰⁰ (אולי זה גמדי).

"אם יעשו פעם משאל בין מתמטיקאים, מתי המורה היפה ביותר, כנראה שמתגלגל גלואה תרצה בהפרש גדול.

נצרת היא במידה מסוימת משהו שנכפה עלינו על ידי האב. אלגברה היא מורה שפיתחה מאעמים אסתטיים."

למי מוסימיות מרכזית הובילו לפיתוח מרגל גלואה: בניית הסדרה ובמחשבה, ופיתוח משוואה (פולינומילית).

(שלוש בעיות חשובות לא הוציחו היווניים לפתור באמצעות סדרה ומחשבה: חלוקת זווית לשלוש, הכפלה הקוביה וריבוע המעגל.

(השיטה לפתרון משוואה ריבועית הייתה ידועה מימי הבבלים, השיטה לפתרון משוואות ממעלה שלישית וריבועית פותחו בסביבות 1500, ופיתוחו ע"י קרדן. אך גם לאחר מכן לא הייתה ידועה שיטה לפתרון משוואה ממעלה חמישית.

מרגל גלואה מוכיחה שלא ניתן לפתור עם סדרה ומחשבה את שלושת הבעיות על ידי קדם, ושלא ניתן לפתור באמצעות ניסוח עם רדיקלים (שורשים מכל מעלה) משוואה ממעלה חמישית.

הממצא של מרגל גלואה גרמו גם למחומים נוספים רבים במתמטיקה.

ספרות: כל הספרים של הקורס נקראים "Galois Theory" כל אחד

מהם נכתב על ידי סופר אחר:

* David Cox

* J. Rotman

* I. Stewart

המסמן הוא המרכזי בקורס, והבחור ביותר.

חוקים

הצגה: R הינה קבוצה בה מוגדרות שתי פעולות: חיבור (+) וכפל ($\cdot$), כך ש- R הינה חבורה חילופית ביחס לחיבור, והכפל אסוציאטיבי. כמו כן, מתקיים חוק הפילוג:

$$a(b+c) = ab+ac, \quad (a+b)c = ac+bc$$

אם קיים איבר יחידה 1 בחוג (כלל a),
נאמר כי R הוא חוג עם יחידה.
אם לכל $a, b \in R$ מתקיים $ab=ba$ אז נאמר כי R הוא חוג חילופי.

דוגמאות: (1) $\mathbb{Z}$ - חוג השלמים, זהו חוג חילופי עם יחידה,

(2) $M_n(F)$ - מטריצות $n \times n$ מעל שדה F .
זהו חוג עם יחידה שאינן חילופי.

(3) $F[x]$ - אגס של הפולינומים במשתנה אחד מעל שדה F .
זהו חוג חילופי עם יחידה,

(4) שדה - זהו חוג חילופי עם יחידה, כך שלכל $a \in R, a \neq 0$ יש איבר הופכי b (כלומר, $a \cdot b = 1$).

אם בחוג R קיימים a, b כך ש:
נאמר כי R הינו חוג עם מתקי אפס.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

דוגמה: $M_n(F)$ הוא חוג עם מתקי אפס:

$$na = \underbrace{a + \dots + a}_n$$

סימון: אם a אינו בחוג, $n \in \mathbb{Z}$, $(n)a$

הצגה: יהיו R_1, R_2 חוגים. הסתק $f: R_1 \rightarrow R_2$ תקרא הומומורפיזם של חוגים אם לכל $x, y \in R_1$ מתקיים:

$$f(x+y) = f(x) + f(y), \quad f(xy) = f(x) \cdot f(y)$$

אם f חתום ושל נאמר כי f איזומורפיזם, ו- R_1, R_2 איזומורפיים.
הצגה: יהי $f: R_1 \rightarrow R_2$ הסתקה של חוגים (משכיו, "הסתקה" היא הומומורפיזם), נגדיו את התדוף של f אפיון:

$$\ker f = \{x \in R_1 : f(x) = 0\}$$

אמנה: $\ker f$ הינה תת-חבורה חבורה של R_1 . הנוסף מתקיים: אם $a \in \ker f$ ו- $r \in R_1$, אז $f(ra) = f(r)f(a) = 0$ כלומר, $ra, ra \in \ker f$.

הגדרה: יהי R חוג. תת-קבוצה $I \subseteq R$ נקרא אידיאל אם I הינה תת-חבורה חיבורית של R והיא סגורה תחת כפל של איברים ב- R משמאל ומימין.

דוגמאות: 1. סדרתן של ~~מספרים~~ הומומורפיזם הוא אידיאל.

2. נחלק את האידיאלים בחוג $F[x]$. יהי I אידיאל כלשהו השונה מאפס. יהי $g(x)$ איבר ב- I שדרגתו * מינימלית. נראה כי:

$$I = \{f(x)g(x) : f(x) \in F[x]\} = \langle g(x) \rangle$$

יהי $h(x) \in I, h(x) \neq 0$, נחלק עם שארית ונקבל:

$$h(x) = q(x)g(x) + r(x)$$

כאשר דרגת $r(x)$ קטנה ממש מדרגת $g(x)$. אבל:

$$r(x) = h(x) - q(x)g(x) \in I$$

מינימליות הדרגה של $g(x)$ בפולינום ב- I נקבל $r(x) = 0$.

לכן $h(x) = q(x)g(x)$. זה מה שרצינו להוכיח. $\square$

הגדרה: חוג חילופי שצורתו כל אידיאל נוצר על ידי איבר יחיד, כלומר כל אידיאל הוא מכלול $\langle a \rangle$, $a \in R$, נקרא חוג ראשי, או

pid; principal ideal domain

דוגמה: $\mathbb{Z}$ (או למעשה, כל חוג שיש בו חילוק עם שארית).

הגדרה: יהי R חוג ויהי $I \subseteq R$ אידיאל. אז R/I הינה חבורה חיבורית שאיבריה הם $a+I$, $a \in R$, נגדיר כפל על-ידי:

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

כפל זה מוגדר היטב כי I הינו אידיאל. בצורה זו נקבל כי R/I הינו חוג. אם R חילופי אז R/I חילופי. אם R עם איבר יחידה 1 , אז $1+I$ הינו איבר יחידה ב- R/I .

R/I נקרא חוג חתך.

ההצגה $R/I \rightarrow R$ ψ המוגדרת ע"י $\psi(x) = x+I$ הינה ההצגה של חטים והיא ההצגה של.

הגדרה: תת-קבוצה $S \subseteq R$ נקרא תת-חוג אם S היא חוג עם הפעולות של R .

אינטואיציה חשובה: תת-חוג אנלוגי לתת-חבורה במורה החבורות. אידיאל אנלוגי לתת-חבורה נורמלית.

* דן הן היה מעיר, שהמונח הנכון הוא "מעלה" ולא "דרגה".

(1) $f: R_1 \rightarrow R_2$ הפסקה על חוגים, $\ker f \cong \text{Im } f$

(2) R חוג, $S \subseteq R$ תת-חוג ו- $I \subseteq R$ אידיאל.
 $\ker f \cong \text{Im } f$

$$\frac{S}{I \cap S} \cong \frac{S+I}{I}$$

לענין: $I \subseteq R$ אידיאל בחוג R עם יחידה, אם I מכיל איבר

הפסקה $I = R$ (א) הפסקה R אם קיים $b \in R$ כך ש: $ab=1$

הוכחה: אם $a \in I$ הפסקה, $1 = a^{-1}a \in I$

לכן, לכל $x \in R$, $x = x \cdot 1 \in I$, מכאן $I = R$. $\square$

הערה: $I \subseteq R$ "קטן מקסימלי" אם $I \subset R$ (אם I מכיל a אז $I = R$)
 ולא קיים אידיאל J המכיל I ומהפך R ומהפך I .

מעבר, נבדוק את החוגים חסומים עם יחידה, אבל אם R/I שדה.

לענין: $I \subseteq R$ אידיאל מקסימלי, R/I שדה.
הוכחה: R/I אידיאל מקסימלי, ויהי $a \notin I$. אם האידיאל הנוצר
 על ידי a ו- I , $\langle I, a \rangle$, מכיל 1 ומהפך R ולכן $\langle I, a \rangle = R$.
 לכן קיים $r \in R$, $i \in I$, כך ש: $ra+i=1$ (כל איבר
 ב- $\langle I, a \rangle$ הוא מהצורה $ra+i$). בחוג R/I נקבל את השוויון:
 $(r+I)(a+I) = ra+I = 1+I$. לכן $r+I$ הוא ההפסקה של $a+I$.
 מכאן R/I שדה.

לכן, אם R/I שדה אז I אידיאל מקסימלי, $a \notin I$, הפסקה $a+I$ לכן שדה R/I .
 $\square$ $a \notin I$ נקבל $\langle I, a \rangle = R$ $I \subseteq R$ מקסימלי.