תורת החוגים - טענות בלבד

מבנים אלגבריים (2) - 80446

מרצה: שי אברה

מתרגל: אור רז

סוכם ע"י שריה אנסבכר

סמסטר ב' תשפ"ד, האוניברסיטה העברית

תוכן העניינים

בהכנת סיכום זה נעזרתי רבות בספר "מבנים אלגבריים" מאת: דורון פודר, אלכס לובוצקי ואהוד דה-שליט.

* * *

סביר להניח שהסיכומים שלי מכילים טעויות רבות - אני מוצא כאלה כל יום (רשימת טעויות נפוצות),
אני מפציר בכם לעדכן אותי בכל טעות שאתם מוצאים (ממש כל טעות ללא יוצא מן הכלל);
אתם מוזמנים להגיב על המסמכים ב-Google Drive, לשלוח לי דוא"ל או למלא פנייה באתר.

לסיכומים נוספים היכנסו לאתר:
אקסיומת השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 חוגים כלליים

יהי R חוג.

1.1 התחלה

משפט 1.1. לכל $a\in R$ מתקיים $a\cdot 0=0\cdot a=0$.

מסקנה 1.2. אם יש ב-R שני איברים שונים אז $1\neq 0$ (כמובן שגם הכיוון ההפוך נכון).

משפט 1.3. יחידות האיבר האדיש לחיבור
יהיו $a,b\in R$, אם $a+b=a$ אז $b=0$.

מסקנה 1.4. יחידות הנגדי
יהיו $a,b,c\in R$, אם $a+b=0$ וגם $a+c=0$ אז $b=c$.

- ♣ בגלל מסקנה זו יש משמעות לסימון $-a$ עבור $a\in R$.
- ♣ מתקיים $-0=0$.

משפט 1.5. לכל $a\in R$ מתקיים $a\cdot 1=1\cdot a=a$.

טענה 1.6. לכל $a,b\in F$ מתקיימים כל הפסוקים הבאים:

1. $-(-a)=a$.
2. $(-1)\cdot a=-a$.
3. $a\neq 0$ אם"ם $-a\neq 0$.
4. $a=b$ אם"ם $a-b=0$.
5. $-(a+b)=-a-b$.
6. $-(a-b)=b-a$.
7. $(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$.
8. $(-a)\cdot(-b)=a\cdot b$.

1.2 אידיאלים

טענה 1.7. יהי $I\trianglelefteq R$ אידיאל, אם יש ב-I איבר הפיך ($I\cap R^\times\neq\emptyset$) אז $I=R$.

טענה 1.8. יהי $I\trianglelefteq R$ אידיאל, I מקסימלי אם"ם R/I הוא חוג פשוט.

משפט 1.9. לכל אידיאל $I\trianglelefteq R$ כך ש-$I\neq R$ קיים אידיאל מקסימלי $M\trianglelefteq R$ כך ש-$I\subseteq M$.

טענה 1.10. תהא X קבוצת אידיאלים של R, החיתוך של כל האידיאלים ב-X הוא אידיאל של R, וזהו האידיאל הגדול ביותר (ביחס להכלה) שמוכל בכל האידיאלים ב-X.

♣ נשים לב לכך שיש כאן כמה אפשרויות:

- X יכולה להיות סופית ואז קיימים אידיאלים $I_1, I_2, \ldots, I_r \subseteq R$ כך ש-$X = \{I_1, I_2, \ldots, I_r\}$, ואז החיתוך של כל האידיאלים בה הוא הקבוצה:
$$\bigcap_{i=1}^{r} I_i$$
- X יכולה להיות אין-סופית בת-מנייה, כלומר ניתן לסדר את איבריה בסדרה אינסופית: $X = \{I_1, I_2, \ldots\}$ ואז החיתוך של כל האידיאלים בה הוא הקבוצה:
$$\bigcap_{i=1}^{\infty} I_i$$
- X יכולה להיות אין-סופית שאינה בת-מנייה, כלומר א"א לסדר את איבריה בסדרה אינסופית, ואז החיתוך של כל האידיאלים בה הוא הקבוצה:
$$\bigcap_{I \in X} I$$

בכל מקרה החיתוך של כל האידיאלים ב-X הוא הקבוצה:
$$\left\{\ r \in R \ \middle|\ \forall I \in X : r \in I\ \right\}$$

טענה 1.11. תהא $S \subseteq R$ תת-קבוצה, מתקיים:
$$(S) = \left\{\ \sum_{i=1}^{n} a_i \cdot s_i \cdot b_i \ \middle|\ n \in \mathbb{N},\ \ \forall n \geq i \in \mathbb{N}\ \ s_i \in A \wedge a_i, b_i \in R\ \right\}$$
ואם R הוא חוג חילופי אז גם:
$$(A) = \left\{\ \sum_{i=1}^{n} a_i \cdot s_i \ \middle|\ n \in \mathbb{N}_0,\ \ \forall n \geq i \in \mathbb{N}\ \ s_i \in A \wedge a_i \in R\ \right\}$$

טענה 1.12. יהיו $I, J \trianglelefteq R$ שני אידיאלים, הקבוצה $I + J = \{i + j \mid i \in I,\ \ j \in J\}$ גם היא אידיאל, וזהו האידיאל הקטן ביותר (ביחס להכלה) שמכיל הן את I והן את J.

טענה 1.13. לכל שני אידיאלים $I, J \trianglelefteq R$, הקבוצה $IJ := \{\sum_{i=1}^{n} x_i \cdot y_i \mid n \in \mathbb{N}_0,\ \ \forall n \geq i \in \mathbb{N}\ \ x_i \in I \wedge y_i \in J\}$ גם היא אידיאל.

אני מנחש ששלוש הטענות האחרונות נכונות גם עבור אידיאלים ימניים/שמאליים (בנפרד כמובן).

2 הומומורפיזמים

יהי R חוג.

2.1 התחלה

טענה 2.1. הרכבה של הומומורפיזמים היא הומומורפיזם, והרכבה של איזומורפיזמים היא איזומורפיזם.

מסקנה 2.2. $\mathrm{Aut}\left(R\right)$ היא חבורה ביחס לפעולת ההרכבה.

טענה 2.3. יהיו S חוג ו-$\varphi:R\to S$ הומומורפיזם.
מתקיים $\ker\varphi\trianglelefteq R$ ו-$\mathrm{Im}\varphi\leqslant S$; כלומר $\ker\varphi$ הוא **אידיאל** של R, ו-$\mathrm{Im}\varphi$ הוא **תת-חוג** של S.

♣ טענה זו לא הייתה נכונה אם לא היינו דורשים ש-$\varphi\left(1_{R}\right)=1_{S}$, שכן אז העתקת האפס הייתה נחשבת הומומורפיזם ותמונתה לא הייתה תת-חוג של הטווח.

מסקנה 2.4. כל הומומורפיזם הוא אפימורפיזם ביחס לתמונתו, וכמו כן כל מונומורפיזם הוא איזומורפיזם בין תחום ההגדרה שלו לתמונתו.

למה 2.5. יהי $I\trianglelefteq R$ אידיאל, פונקציית ההטלה של I (כתת-חבורה חיבורית של R) היא הומומורפיזם.

מסקנה 2.6.

- תת-קבוצה $S\subseteq R$ היא תת-חוג של R אס"ם היא תמונה של הומומורפיזם.
- תת-קבוצה $I\subseteq R$ היא אידיאל של R אס"ם היא גרעין של הומומורפיזם.

משפט 2.7. **"משפט קיילי לחוגים"**[1]
קיימת חבורה אבלית A כך ש-R ניתן לשיכון ב-$\mathrm{End}\left(A\right)$, כלומר R איזומורפי לתת-חוג של $\mathrm{End}\left(A\right)$.

2.2 משפטי האיזומורפיזם לחוגים

משפט 2.8. **משפט האיזומורפיזם הראשון**
יהיו S חוג ו-$\varphi:R\to S$ הומומורפיזם, מתקיים:

$$R/\ker\varphi\cong\mathrm{Im}\varphi$$

מסקנה 2.9. **משפט האיזומורפיזם השני**
יהיו $S\leqslant R$ תת-חוג ו-$I\trianglelefteq R$ אידיאל; מתקיים $S\cap I\trianglelefteq S$ ו-$S+I\leqslant R$, ובנוסף:

$$S+I/I\cong S/S\cap I$$

משפט 2.10. **משפט האיזומורפיזם השלישי**
יהיו $I,J\trianglelefteq R$ אידיאלים כך ש-$I\subseteq J$, מתקיים:

$$\left(R/J\right)/\left(J/I\right)\cong R/I$$

[1] ערך בוויקיפדיה: קיילי ארתור.

משפט 2.11. משפט ההתאמה[2]

יהי $I \trianglelefteq R$ אידיאל ונסמן ב-π את הומומורפיזם ההטלה הקנוני של I.

קיימת התאמה משמרת הכלה, חח"ע ועל, בין תתי-חוגים של R המכילים את I לבין תתי-חוגים של ${}^{R}/_{I}$. התאמה זו היא הפונקציה $f:\{S\leqslant R\mid I\subseteq S\}\to\{L\mid L\leqslant {}^{R}/_{I}\}$ המוגדרת ע"י (לכל $S\leqslant R$ כך ש-$I\subseteq S$)[3]:

$$f(S):={}^{S}/_{I}={}^{S+I}/_{I}=\pi(S)$$

כמו כן קיימת התאמה משמרת הכלה, חח"ע ועל, בין אידיאלים של R המכילים את I לבין אידיאלים של ${}^{R}/_{I}$. התאמה זו היא הפונקציה $g:\{J\trianglelefteq R\mid I\subseteq I\}\to\{L\mid L\trianglelefteq {}^{R}/_{I}\}$ המוגדרת ע"י (לכל $J\trianglelefteq R$ כך ש-$I\subseteq J$):

$$g(J):=\pi(J)$$

כלומר משפט ההתאמה טוען כי:

- f הנ"ל היא פונקציה חח"ע ועל (כלומר הפיכה, ההופכית שלה מוגדרות ע"י $f^{-1}(L):=\pi^{-1}(L)$[4] לכל $S\leqslant {}^{R}/_{I}$), ולכל $I\leqslant S,K\leqslant G$ מתקיים:
$$K\leqslant S\iff {}^{K}/_{I}=f(K)\leqslant f(S)={}^{S}/_{N}$$
- g הנ"ל היא פונקציה חח"ע ועל (כלומר הפיכה, ההופכית שלה מוגדרות ע"י $g^{-1}(L):=\pi^{-1}(L)$ לכל $J+I\trianglelefteq {}^{R}/_{I}$), ולכל $I\leqslant J,K\leqslant G$ מתקיים:
$$K\subseteq J\iff g(K)\trianglelefteq g(J)$$

3 חוגים חילופיים (קומוטטיביים)

יהי R חוג חילופי שאינו טריוויאלי.

3.1 יחס החלוקה

טענה 3.1. לכל $a,b\in R$ מתקיים $(b)\subseteq(a)\iff a\mid b$.

טענה 3.2. יהיו $a,b\in R$, התנאים הבאים שקולים:

1. a ו-b חברים.
2. $(a)=(b)$.
3. קיים איבר הפיך $r\in R^{\times}$ כך ש-$a=r\cdot b$.

טענה 3.3. איבר לא הפיך $0\neq r\in R$ הוא אי-פריק אם"ם לכל $a\in R$ כך ש-$(r)\subseteq(a)$ מתקיים $(a)=(r)$ או ש-$(a)=R$.

טענה 3.4. R הוא שדה אם"ם הוא חוג פשוט.

מסקנה 3.5. יהי $I\trianglelefteq R$ אידיאל, ${}^{R}/_{I}$ הוא שדה אם"ם I הוא אידיאל מקסימלי.

משפט השאריות הסיני לחוגים

[2] יש המכנים משפט זה בשם "משפט האיזומורפיזם הרביעי", למרות שבעצם אין בו איזומורפיזם בין חוגים.

[3] נזכיר ש-π היא פונקציה מ-R ל-${}^{R}/_{I}$ (תחום ההגדרה שלה אינו זה של f), ופירושו של הסימון "$\pi(S)$" הוא $\{\pi(s)\mid s\in S\}$.

[4] גם כאן נזכיר ש-π כלל אינו מוכרח להיות הפיך, פירושו של הסימון "$\pi^{-1}(L)$" הוא $\{r\in R\mid\pi(r)\in L\}$.

טענה 3.6. יהיו $a_1, a_2, \ldots, a_n \in R$ שלפחות אחד מהם שונה מ-0, ונסמן $I := (a_1, a_2, \ldots, a_n)$ (כלומר I הוא האידיאל הנוצר ע"י $a_1, a_2, \ldots, a_n$).
איבר $d \in R$ הוא מחלק משותף מקסימלי של $a_1, a_2, \ldots, a_n$ אם"ם מתקיימים שני התנאים הבאים:

1. $I \subseteq (d)$.
2. לכל $\tilde{d} \in R$ כך ש-$I \subseteq \left(\tilde{d}\right)$ מתקיים $(d) \subseteq \left(\tilde{d}\right)$.

3.2 תחומי שלמות

טענה 3.7. יהי $I \trianglelefteq R$ אידיאל, I הוא אידיאל ראשוני אם"ם R/I הוא תחום שלמות.

מסקנה 3.8. כל אידיאל מקסימלי ב-R הוא אידיאל ראשוני.

נניח ש-R הוא תחום שלמות.

סימון: נסמן $X := \left\{(a,b) \in R^2 \mid b \neq 0\right\}$ ונגדיר על X את היחס הבא[5]:

$$(a,b) \sim (c,d) \iff ad = bc$$

למה 3.9. היחס הנ"ל הוא יחס שקילות.

סימון: נסמן ב-$\frac{a}{b}$ את מחלקת השקילות של (a,b) לכל $(a,b) \in X$, כמו כן נסמן:

$$Q := \left\{ \ \frac{a}{b} \ \middle| \ a,b \in R, \ \ b \neq 0 \ \right\}$$

ונגדיר על Q פעולות חיבור וכפל ע"י (לכל $\frac{a}{b}, \frac{c}{d} \in Q$):

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} := \frac{a \cdot c}{b \cdot d}$$

♣ כמובן שיש לבדוק שהפעולות מוגדרות היטב ולא תלויות בבחירת הנציגים.

למה 3.10. Q הוא שדה ביחס לפעולות החיבור והכפל הנ"ל, כאשר האיבר האדיש לחיבור הוא $\frac{0}{1}$ והאיבר האדיש לכפל הוא $\frac{1}{1}$.

מסקנה 3.11. R ניתן לשיכון בתוך Q, כלומר קיים מונומורפיזם $\varphi : R \to Q$.

♣ כמובן שהשיכון הפשוט ביותר הוא $r \mapsto \frac{r}{1}$.

מסקנה 3.12. חוג ניתן לשיכון בשדה אם"ם הוא תחום שלמות.

טענה 3.13. יהי $\mathbb{F}$ שדה, לכל מונומורפיזם $\varphi : R \to \mathbb{F}$ קיים מונומורפיזם $\hat{\varphi} : Q \to \mathbb{F}$ כך ש-$\hat{\varphi} \mid_R = \varphi$.

משפט 3.14. כל תחום שלמות סופי הוא שדה.

3.3 תחומי פריקות חד-ערכית

נניח ש-R הוא תחום פריקות חד-ערכית.

משפט 3.15. איבר $r \in R$ הוא אי-פריק אם"ם הוא ראשוני.

בתחום פח"ע ה-gcd מוגדר לכל שני איברים וניתן להציג אותו ע"י הפירוק לגורמים, ולהסיק מכאן כיצד נראה גם ה-lcm.

[5] פורמלית $\sim := \left\{((a,b),(c,d)) \in X^2 \mid ad = bc\right\}$

3.4 תחומים ראשיים

משפט 3.16. כל תחום ראשי הוא תחום פריקות חד-ערכית.

נניח ש-R הוא תחום ראשי.

טענה 3.17. איבר $0 \neq r \in R$ הוא אי-פריק/ראשוני אם"ם (r) הוא אידיאל מקסימלי.

מסקנה 3.18. לכל אידיאל $\{0\} \neq I \trianglelefteq R$ מתקיים: I הוא אידיאל מקסימלי אם"ם I הוא אידיאל ראשוני.

טענה 3.19. יהיו $a_1, a_2, \ldots, a_n \in R$ שלפחות אחד מהם שונה מ-0, ונסמן $I := (a_1, a_2, \ldots, a_n)$ (כלומר I הוא האידיאל הנוצר ע"י $a_1, a_2, \ldots, a_n$).
יש ל-$a_1, a_2, \ldots, a_n$ מחלק משותף מקסימלי $d \in R$, מתקיים $I = (d)$, וממילא קיימים $x_1, x_2, \ldots, x_n \in R$ כך שמתקיים:

$$d = x_1 \cdot a_1 + x_2 \cdot a_2 + \ldots + x_n \cdot a_n$$

3.5 חוגים אוקלידיים

משפט 3.20. כל תחום אוקלידי הוא תחום ראשי, ולפיכך גם תחום פריקות חד-ערכית.

נניח ש-R הוא תחום אוקלידי, ונסמן ב-N את הנורמה שלו.

מסקנה 3.21. לכל $\{0\} \neq I \trianglelefteq R$ מתקיים $I = (d)$ לכל $d \in I$ בעל נורמה מינימלית מבין כל האיברים ב-I.

יהיו $r_0, r_1 \in R$ כך שלפחות אחד מהם שונה מאפס, נרצה למצוא מחלק משותף מקסימלי של r_0 ו-r_1.
לאלגוריתם ישנן שתי גרסאות: האלגוריתם הבסיסי והאלגוריתם המורחב, להלן הפירוט של שניהם בפסאודו-קוד.

אלגוריתם 1 אלגוריתם אוקלידס הבסיסי

נגדיר $i := 0$.
כל עוד $r_{i+1} \neq 0$:

- נחלק את r_i ב-r_{i+1} עם שארית, נסמן ב-q_i את המנה וב-r_{i+2} את השארית (כלומר יהיו $q_i, r_{i+2} \in R$ כך ש-> $0 \leq N(r_{i+2})$ $N(r_{i+1})$ או ש-$r_{i+2} = 0$ וגם $r_i = r_{i+1} \cdot q_i + r_{i+2}$).
- נגדיר את i להיות $i+1$ ונעבור לשלב הבא בלולאה.

כעת מתקיים $r_{i+1} = 0$, א"כ r_i הוא מחלק משותף מקסימלי של r_0 ו-r_1, ולכן נחזיר את r_i ונסיים.

אלגוריתם 2 אלגוריתם אוקלידס המורחב

נגדיר $i:=0$.

נגדיר $a_{-1}:=0$ ו-$b_{-1}:=1$ ומכאן שמתקיים:

$$r_1=a_{-1}\cdot r_0+b_{-1}\cdot r_1$$

כל עוד $r_{i+1}\neq 0$:

- נחלק את r_i ב-r_{i+1} עם שארית, נסמן ב-q_i את המנה וב-r_{i+2} את השארית.
- נחלק למקרים:
  - אם $i=0$ אז נגדיר $a_0:=1$ ו-$b_0:=-q_0$.
  - אחרת, נגדיר $a_i=a_{i-2}-q_i\cdot a_{i-1}$ ו-$b_i:=b_{i-2}-q_i\cdot b_{i-1}$.
- נגדיר את i להיות $i+1$ ונעבור לשלב הבא בלולאה.

כעת מתקיים $r_{i+1}=0$, r_i הוא מחלק משותף מקסימלי של r_0 ו-r_1, ובנוסף:

$$\gcd(r_0,r_1)=r_i=a_{i-2}\cdot r_0+b_{i-2}\cdot r_1$$

3.6 חוג פולינומים מעל שדה

♣ ראו גם את הקובץ "פולינומים על".

טענה 3.22. יהי $\mathbb{F}$ שדה, $\mathbb{F}[x]$ הוא חוג אוקלידי.

משפט 3.23. הלמה של גאוס

יהי $f\in\mathbb{Z}[x]$ פולינום, אם f פריק ב-$\mathbb{Q}[x]$ אז הוא פריק גם ב-$\mathbb{Z}[x]$.

♣ הלמה של גאוס נכונה עבור כל תחום פריקות חד-ערכית (במקרה הזה $\mathbb{Z}$) ושדה השברים שלו (במקרה הזה $\mathbb{Q}$).

♣ לא כל פולינום אי-פריק ב-$\mathbb{Z}[x]$ הוא גם אי-פריק ב-$\mathbb{Q}[x]$, אמנם נובע מהמשפט שפולינום כזה אינו פריק ב-$\mathbb{Q}[x]$ אך עדיין לא נובע מזה שהוא אי-פריק משום שישנה אפשרות נוספת - הוא הפיך.

משפט 3.24. אפיון אייזנשטיין[6]

יהי $f\in\mathbb{Z}[x]$ פולינום, נסמן $n:=\deg f$, ויהיו $a_0,a_1,\ldots,a_n\in\mathbb{Z}$ כך ש-$f(x)=\sum_{i=0}^{n}a_i\cdot x^i$.

אם קיים $p\in\mathbb{N}$ ראשוני כך שמתקיים:

1. $p\mid a_i$ לכל $n>i\in\mathbb{N}_0$.
2. p לא מחלק את a_n.
3. p^2 לא מחלק את a_0.

אז f אינו פריק ב-$\mathbb{Z}[x]$.

♣ מהלמה של גאוס נובע שאם $\deg f>0$ אז מהעובדה ש-f אי-פריק ב-$\mathbb{Z}[x]$ נובע שהוא גם אי-פריק ב-$\mathbb{Q}[x]$.

[6] ערך בוויקיפדיה: אייזנשטיין פרדיננד.

4 שדות

יהי $\mathbb{F}$ שדה.

טענה 4.1. אם $\mathrm{char}\left(\mathbb{F}\right)\neq0$ אז $\mathrm{char}\left(\mathbb{F}\right)$ הוא מספר ראשוני.

מסקנה 4.2. $\mathbb{F}_{p}$ ניתן לשיכון בכל שדה ממציין p ראשוני, ו-$\mathbb{Q}$ ניתן לשיכון בכל שדה ממציין 0.

מסקנה 4.3. אם $\mathbb{F}$ סופי אז $\mathrm{char}\left(\mathbb{F}\right)$ הוא מספר ראשוני.

תזכורת: כל שדה הוא מרחב וקטורי מעל כל תת-שדה שלו.

מסקנה 4.4. אם $\mathbb{F}$ סופי אז קיים ראשוני p ו-$e\in\mathbb{N}$ כך ש-$\left|\mathbb{F}\right|=p^{e}$.

למה 4.5. יהי $0\neq f\in\mathbb{F}\left[x\right]$ פולינום ונסמן $n:=\deg f$, חוג המנה $\mathbb{F}[x]/(f)$ הוא מרחב וקטורי מעל $\mathbb{F}$, ו-$\left(1+\left(f\right),x+\left(f\right),\ldots,x^{n-1}+\left(f\right)\right)$ הוא בסיס שלו (בפרט $\dim\left(\mathbb{F}[x]/(f)\right)=n$).

בספר הקורס כתוב ש-f נדרש להיות מתוקן, אין לי מושג למה יש בזה צורך.

מסקנה 4.6. נניח ש-$p:=\mathrm{char}\left(\mathbb{F}\right)\neq0$, יהי $f\in\mathbb{F}\left[x\right]$ פולינום אי-פריק ונסמן $n:=\deg f$; חוג המנה $\mathbb{F}[x]/(f)$ הוא שדה סופי בגודל p^{n-1}.

טענה 4.7. אם $\mathbb{F}$ סופי אז החבורה הכפלית $\mathbb{F}^{\times}$ היא חבורה ציקלית.

תזכורת: כל שדה הוא בפרט חוג, הומומורפיזמים של שדות על שלל סוגיהם הם פשוט הומומורפיזמים של חוגים אלא שהתחום והטווח שלהם הם שדות, בפרט נאמר ששני שדות איזומורפיים זה לזה אם קיים איזומורפיזם של חוגים ביניהם.

משפט 4.8. אם $\mathbb{F}$ סופי אז קיימים p ראשוני ופולינום $f\in\mathbb{F}_{p}\left[x\right]$ אי-פריק (ב-$\mathbb{F}_{p}\left[x\right]$) כך ש-$\mathbb{F}\cong\mathbb{F}_{p}[x]/(f)$.