סיכום מבנים אלגבריים - תשפ"ו 2026

22 במרץ 2026

גיא יער־און

הסיכום נכתב במהלך סמסטר ב' תשפ"ו (2026), ומבוסס על הרצאותיו של ד"ר ארז שיינר, לכן יתכן שנפלו טעויות בסיכום, כך שהשימוש בו על אחריותכם בלבד.

תוכן עניינים

1 הקדמה 1
1.1 חבורה $(Group)$ 1
1.2 חוג $(Ring)$ 2
1.3 שדה $(Field)$ 2
2 חבורות 2
2.1 דוגמאות מרכזיות לחבורות 3

1 הקדמה

מהם מבנים אלגבריים? למעשה, כבר למדנו מבנה אלגברי מסויים בקורס אלגברה לינארית: **שדה**. למשל, $\mathbb{Z}_7$ הוא מופע של שדה. בקורס, נעסוק בעיקר במבנה אלגברי שנקרא **חבורה**, ומעט במבנה אלגברי שנקרא **חוג**. כמו כן, נרחיב על מושג השדה.

אנחנו סטודנטים למדעי המחשב, למה שנלמד קורס מתקדם על מבנים אלגבריים? נלמד בקורס זה על שני שימושים חשובים של מבנים אלגבריים אלו שקשורים לעולם מדעי המחשב:

- הצפנה
- קידוד

מה זה **הצפנה**? אפשר לחשוב על כך **כהסתרה** של מידע, זו המטרה העיקרית של הצפנה. נרצה לדאוג גם ל**אמינות** ו**שלמות** של המידע. למשל: כאשר מייקרוסופט מורידים עדכון גרסה, הוא לא צריך להיות מוסתר - אבל אנחנו צריכים להיות בטוחים שמייקרוסופט הם אלו שכתבו את העדכון, על מנת שלא נוריד בטעות וירוס - זה נקרא אמינות, ושלמות הכוונה היא שלא "יתנקשו" לי במידע ואקבל את כולו.

מה זה **קידוד**? מוסכמה לתבנית להעברת מידע. למשל: "יום ההולדת שלי הוא 2", הכוונה היא שכנראה אפשר להסתכל על כך כיום השני בשנה. שני הצדדים כמובן, צריכים להסכים על הקידוד: אחרת - יהיו לנו כמה וכמה פרשנויות שונות למידע. למשל, אפשר להתייחס למשפט אודות יום ההולדת כ"יום ההולדת שלי הוא בשני לחודש הבא" או "אני בן שנתיים" וכדומה. **פרוטוקול** (פרוטוקול תקשורת הוא סט של חוקים ומוסכמות המגדירים כיצד מכשירים דיגיטליים מעבירים נתונים ביניהם, כדי שיבינו את המידע הנשלח ויגיבו אליו בצורה תקינה.) למשל, הוא סוג של קידוד. בקורס נתמקד בעיקר בזיהוי ותיקון של שגיאות בקידוד ונלמד על RSA (אלגוריתם הצפנה).

האנלוגיה הכי קרובה למבנים אלגבריים מעולם מדעי המחשב, היא תכנות מונחה עצמים ובפרט ממשק (interface).
כפי שאמרנו, נתקלנו בעבר בשדות (מבנה אלגברי) ואף הוכחנו את הטענה הבאה:

משפט 1. יהי שדה $\mathbb{F}$, איבר האפס $0_{\mathbb{F}} \in \mathbb{F}$, ויהי $a \in \mathbb{F}$, אזי מתקיים: $a \cdot 0_{\mathbb{F}} = 0_{\mathbb{F}}$.

1.1 חבורה $(Group)$

הגדרה 2. חבורה היא קבוצה G יחד עם פעולה (בהיעדר מידע נוסף, נשתמש בסימון הכפל) שתסומן $(G, \cdot)$ כך שמתקיימות התכונות הבאות:

1. סגירות: $\forall a, b \in G : a \cdot b \in G$
2. אסוציאטיביות: $\forall a, b, c \in G : (ab)c = a(bc)$
3. ניטרלי (איבר יחידה): $\exists e_G \in G$ המקיים: $\forall a \in G : a \cdot e_G = e_G \cdot a = a$
4. קיום איבר הופכי: $\forall a \in G, \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e_G$

הערה 3. מניטרליות, נקבל כי בהכרח חבורה G לא יכולה להיות ריקה: תמיד קיים איבר ניטרלי. את האיבר הניטרלי נסמן בe_G לרוב.

הערה 4. אנחנו לא דורשים קומוטטיביות (חילופיות) בחבורה.

הגדרה 5. תהי G חבורה עם פעולה $\cdot$. נאמר כי G היא חבורה אבלית / קומוטטיבית / חילופית אם הפעולה $\cdot$ מקיימת את חוק החילוף: כלומר $\forall a,b \in G : ab = ba$.

דוגמה 6. נתבונן ב$G = (\mathbb{N}, +)$. האם מדובר בחבורה? אפילו אם $0 \in G$, אין בחבורה איברים הופכיים. הרי 0 הוא איבר ניטרלי לחיבור, ולכן עבור $2 \in \mathbb{N}$ למשל צריך להתקיים: $2 + 2^{-1} = 0$, כלומר $2^{-1} = -2$, אך $-2 \notin \mathbb{N}$ ולכן לא מדובר בחבורה.

דוגמה 7. לעומת זאת, $G = (\mathbb{Z}, +)$ היא כן חבורה. האיברים ההופכיים הם הנגדיים. מיהו האיבר ההופכי של 0? נבחין כי 0 הוא האיבר ההופכי (ה"נגדי") של עצמו.

דוגמה 8. האם $(\mathbb{Q}, \cdot)$ חבורה? לא! ל0 אין הופכי. אך, $(\mathbb{Q}\backslash\{0\}, \cdot)$ וכן $(\mathbb{Q}, +)$ הן חבורות.

1.2 חוג $(Ring)$

הגדרה 9. חוג הוא קבוצה R עם שתי פעולות (שנקרא להן חיבור וכפל, וכמובן רק נקרא להם כך), כך שמתקיימות התכונות הבאות:

1. $(R, +)$ הוא חבורה אבלית.
2. הכפל סגור, אסוציאטיבי ויש איבר יחידה.
3. פילוג: $\forall a,b,c \in G : (a+b)c = ac + bc = \wedge[a(b+c) = ab + ac]$

הערה 10. נבחין שוויתרנו על חילופיות (קומוטטיביות) ואיבר הופכי עבור הכפל. כיוון שאין חילוף, היינו חייבים לכתוב פעמיים את הפילוג.

דוגמה 11. ישנם שני מופעים מוכרים ביותר לחוג שאינם שדות:

1. $\mathbb{Z}_n$ - חוג השאריות עם פעולות מודלו n.
2. **המטריצות הריבועיות מסדר** n - החיבור טוב כחבורה, אך הכפל לא חילופי ולא כל המטריצות הפיכות! נראה כי חוג בדיוק מתאים עבור עולם המטריצות.

1.3 שדה $(Field)$

הגדרה 12. **שדה** הוא קבוצה $\mathbb{F}$ עם שתי פעולות (להן נקרא חיבור וכפל) כך שמתקיימות התכונות הבאות:

1. $(\mathbb{F}, +)$ היא חבורה אבלית.
2. $(\mathbb{F}\backslash\{0\}, \cdot)$ היא חבורה אבלית.
3. פילוג: $\forall a,b,c \in \mathbb{F} : a(b+c) = ab + ac$

הערה 13. נשים לב להבדל בין שדה לחבורה - בחבורה אנחנו דורשים שלכולם יש הופכי, בשדה לכולם פרט לאפס יש הופכי. לכן השדה ללא אפס הוא אכן חבורה.

הערה 14. האם צריך לומר במפורש כי $1 \neq 0$? לא, שהרי $1 \in \mathbb{F}\backslash\{0\}$ ולכן $1 \neq 0$.

הערה 15. כל שדה הוא בפרט חוג (גם זה מזכיר OOP - הורשה).

2 חבורות

משפט 16. (תכונת הצמצום) תהי חבורה G ויהיו $a,b,c \in G$ כך ש$ab = ac$. אזי, בהכרח $b = c$.
הוכחה: G חבורה וכן $a \in G$ לכן קיים לa איבר הופכי, a^{-1}, נכפול בשני הצדדים משמאל ונקבל:

$$a^{-1}(ab) = a^{-1}(ac) \Longrightarrow_* (a^{-1}a)b = (a^{-1}a)c \Longrightarrow eb = ec \Longrightarrow b = c$$

$*$ נכון בגלל אסוציאטיביות. כנדרש.

■

הערה 17. תכונת הצמצום לא נכונה בשדה, כיוון שעבור $a = 0$ זה כמובן לא נכון. כאן, בחבורה, בהכרח לכל איבר קיים נגדי ולכן הטענה כן נכונה. למעשה בשדה הטענה נכונה עבור $a \neq 0$.

הערה 18. כאשר ייאמר לנו החבורה $\mathbb{R}$ או החבורה $\mathbb{Z}$ - אנחנו ישר נניח כי מדובר בחבורה ביחס לפעולת החיבור. מדוע? כי $(\mathbb{R}, \cdot)$ איננו חבורה! שכן עם פעולת הכפל אין הפיכות וכו'.

הערה 19. **סימון:** את $a \cdot a \cdot .... \cdot a$ נסמן a^n.

הערה 20. החבורה הטריוואלית תסומן $(\{e\}, ^*\}$ כאשר $*$ היא פעולה. מדובר בחבורה אבלית!

2.1 דוגמאות מרכזיות לחבורות

משפט 21. נגדיר את S_n להיות אוסף הפונקציות ההפיכות $f:\{1,...,n\}\to\{1,....,n\}$ עם פעולת ההרכבה. אזי, $(S_n,\circ)$ היא חבורה.
הוכחה: נוכיח שאכן מדובר בחבורה. לכן, נעבור תכונה תכונה:
1. **סגירות:** תהיינה $f,g\in S_n$ שתי פונקציות הפיכות. נרצה להראות כי $fg=f\circ g\in S_n$. לפי בדיקה, הרכבת הפיכות היא פונקציה הפיכה כנדרש.
2. **אסוציאטיביות:** תהיינה $f,g,h\in S_n$. הרי, שוב לפי בדיקה הרכבת פונקציות היא פעולה אסוציאטיביות ולכן $(fg)h=f(gh)$
3. **ניטרלי:** פונקציית הזהות $Id\in S_n$ כי הפיכה ומקיימת לכל $f\in S_n$ כי: $f\circ Id=Id\circ f=f$
4. **קיום איבר הופכי:** תהי $f\in S_n$, אזי קיימת לf פונקציה הופכית ונסמנה f^{-1} (והרי בבירור ההופכית היא הפיכה בעצמה) והרי בבירור לפי בדיקה מתקיים $f\circ f^{-1}=f^{-1}\circ f=Id$.

■

הערה 22. באופן כללי קבוצת כל הפונקציות מקבוצה A לעצמה ההפיכות, היא חבורה. עבור קבוצה A נסמן חבורה זו בS_A.

משפט 23. נגדיר את הקבוצה הבאה:

$$GL_n(\mathbb{F})=\{A\in\mathbb{F}^{n\times n}:|A|\neq 0\}$$

כלומר, קבוצת כל המטריצות ההפיכות. אזי, $(GL_n(\mathbb{F}),\cdot)$ היא חבורה.
הוכחה: נוכיח שאכן מדובר בחבורה. לכן, נעבור תכונה תכונה:
1. **סגירות:** תהיינה $A,B\in GL_n(\mathbb{F})$. אזי, כפל מטריצות הפיכות היא מטריצה הפיכה לפי לינארית 1 ולכן אכן $AB\in GL_n(\mathbb{F})$.
2. **אסוציאטיביות:** כפל מטריצות כמובן אסוציאטיבי.
3. **ניטרלי:** מטריצת הזהות I מקיימת לכל $A\in GL_n(\mathbb{F})$ כי: $AI=IA=A$.
4. **קיום איבר הופכי:** תהי $A\in GL_n(\mathbb{F})$. אזי, כיוון שA הפיכה קיימת לה הופכית A^{-1} שגם היא הפיכה. מכאן, מתקיים: $AA^{-1}=A^{-1}A=I$.

■

הערה 24. $(GL_n(\mathbb{F}),+)$ איננה חבורה! $I,-I$ הן הפיכות אך $I+(-I)$ אינה הפיכה. אין סגירות (וחסר עוד הרבה תכונות).

משפט 25. יהי $\mathbb{F}$ שדה. נסמן ב$M_n(\mathbb{F})$ את המטריצות מגודל $n\times n$ מעל $\mathbb{F}$. אזי, $(M_n(\mathbb{F}),\cdot)$ היא חבורה אבלית.

הגדרה 26. תהי G חבורה. המרכז של G הוא:

$$Z(G)=\{x\in G|\forall y\in G:xy=yx\}$$

כלומר, מרכז החבורה הוא קבוצת האיברים בחבורה שמתחלפים עם כולם.

משפט 27. G היא חבורה אבלית $\iff Z(G)=G$

הערה 28. תמיד מתקיים $e_G\in Z(G)$.

הגדרה 29. תהי X קבוצה ונגדיר S_X להיות קבוצת כל התמורות (פונקציות חח"ע ועל) על X. מדובר בחבורה. לכל קבוצה מגודל $|X|\geq 3$, S_X היא חבורה לא אבלית.