מערך תרגיל קורס 88-211 סמסטר א' תשע"ו
אלגברה מופשטת

אוקטובר 2015, גרסה 0.1

מבוא

נתחיל עם כמה דגשים:

- דף הקורס נמצא באתר www.math-wiki.com.
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- חשוב לפתור את תרגילי הבית (אין חובת הגשה, אבל יהיו בחנים שיתבססו עליהם).
- נשמח לכל הערה על מסמך זה.

תרגול 1 מבנים אלגבריים בסיסיים

נפתח בהגדרות לכמה מבנים אלגבריים. מבנה אלגברי שמכירים כבר באלגברה לינארית הוא שדה. אנו נגדיר כמה מבנים יותר "פשוטים", כשהחשוב שבהם הוא חבורה. במרבית הקורס נתרכז בחקר חבורות.

הגדרה 1.1. תהי S קבוצה. פעולה בינארית (binary operation) על S היא פונקציה דו־מקומית $* : S\times S \to S$. עבור $a,b\in S$ כמעט תמיד במקום לרשום $*(a,b)$ נשתמש בסימון $a*b$. מפני שתמונת הפונקציה $a*b$ שייכת ל-S, נאמר כי הפעולה היא סגורה.

הגדרה 1.2. חבורה למחצה (semigroup) היא מערכת אלגברית $(S,*)$ המורכבת מקבוצה לא ריקה S ומפעולה בינארית על S המקיימת קיבוציות (אסוציטיביות, associativity). כלומר לכל $a,b,c\in S$ מתקיים $(a*b)*c=a*(b*c)$.

צורת רישום 1.3. לעיתים נקצר ונאמר כי S היא חבורה למחצה מבלי להזכיר במפורש את המערכת האלגברית. כנ"ל למבנים האלגבריים האחרים.

הגדרה 1.4. תהי $(S,*)$ חבורה למחצה. איבר $e \in S$ נקרא איבר יחידה אם לכל $a \in S$ מתקיים $a * e = e * a = a$. חבורה למחצה שבה קיים איבר יחידה נקראת מונואיד (monoid, או יחידון).

הערה 1.5. יהי M מונואיד. קל לראות כי איבר היחידה ב-M הוא יחיד. הרי אם $e, f \in M$ הם איברי יחידה, אז מתקיים $e = e * f = f$.

הגדרה 1.6. יהי $(M,*,e)$ מונואיד. איבר $a \in M$ יקרא הפיך משמאל אם קיים איבר $b \in M$ כך ש-$ba = e$. במקרה זה b יקרא הופכי שמאלי של a.
באופן דומה, איבר $a \in M$ יקרא הפיך מימין אם קיים איבר $b \in M$ כך ש-$ab = e$. במקרה זה b יקרא הופכי ימני של a.
איבר יקרא הפיך אם קיים איבר $b \in M$ כך ש-$ba = ab = e$. במקרה זה b יקרה הופכי של a.

תרגיל 1.7. יהי $a \in M$ איבר הפיך משמאל ומימין. הראו ש-a הפיך וההופכי שלו הוא יחיד.

פתרון. יהי b הופכי שמאלי כלשהו של a (קיים כזה כי a הפיך משמאל), ויהי c הופכי ימני כלשהו של a (הצדקה דומה). נראה כי $b = c$ ונסיק שאיבר זה הוא הופכי של a. ודאו כי אתם יודעים להצדיק כל אחד מן המעברים הבאים:

$$c = e * c = (b * a) * c = b * (a * c) = b * e = b$$

לכן כל ההופכיים הימניים וכל ההופכיים השמאליים של a שווים זה לזה. מכאן גם שההופכי הוא יחיד, ויסומן a^{-1}.
שימו לב שאם איבר הוא רק הפיך מימין ולא משמאל, אז יתכן שיש לו יותר מהופכי ימני אחד (וכנ"ל בהיפוך הכיוונים)!

תרגיל 1.8 (אם יש זמן)**.** אם $aba \in M$ הפיך במונואיד, הראו כי גם a, b הפיכים.

פתרון. יהי c ההופכי של aba. כלומר

$$abac = caba = e$$

לכן cab הוא הופכי שמאלי של a, ו-bac הופכי ימני של a. בפרט a הפיך ומתקיים $cab = bac$. לכן מתקיים גם

$$(aca)b = a(cab) = a(bac) = e = (cab)a = (bac)a = b(aca)$$

וניתן להסיק כי aca הופכי שמאלי וימני של b.

הגדרה 1.9 חבורה (group) $(G,*,e)$ היא מונואיד שבו כל איבר הוא הפיך. מתקיים: חבורה $\Leftarrow$ מונואיד $\Leftarrow$ חבורה למחצה.

לפי ההגדרה לעיל על מנת להוכיח שמערכת אלגברית היא חבורה צריך להראות:

1. סגירות הפעולה.
2. קיבוציות הפעולה.
3. קיום איבר יחידה.
4. כל איבר הוא הפיך.

הערה 1.10. עבור קבוצה סופית אחת הדרכים להגדיר פעולה בינארית היא בעזרת לוח כפל. למשל, אם $S = \{a, b\}$ ונגדיר

$*$	a	b
a	b	b
b	b	a

אז קל לראות שמתקיימת סגירות, אבל הפעולה אינה קיבוצית כי $(a*b)*b = b*b = a$, אבל $a*(b*b) = a*a = b$.

נסמן כמה קבוצות של מספרים:

- $\mathbb{N} = \{1, 2, 3, \dots\}$ המספרים הטבעיים.
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ המספרים השלמים (מגרמנית: Zahlen).
- $\mathbb{Q} = \left\{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\}\right\}$ המספרים הרציונליים.
- $\mathbb{R}$ המספרים הממשיים.
- $\mathbb{C}$ המספרים המרוכבים.

מתקיים $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

דוגמה 1.11. המערכת $(\mathbb{N}, +)$ של מספרים טבעיים עם החיבור הרגיל של מספרים טבעיים היא חבורה למחצה.

דוגמה 1.12. תהי X קבוצה כלשהי, ותהי $P(X)$ קבוצת החזקה שלה (זהו אוסף כל תתי הקבוצות של X). אזי $(P(X), \cap)$ היא מונואיד שבו איבר היחידה הוא X. מה קורה עבור $(P(X), \cup)$? (להמשך, נשים לב כי במונואיד זה לכל איבר a מתקיים $a^2 = a$.)

דוגמה 1.13. המערכת $(\mathbb{Z}, +)$ היא חבורה שאיבר היחידה בה הוא 0. בכתיב חיבורי מקובל לסמן את האיבר ההופכי של a בסימון $-a$. כתיב זה מתלכד עם המושג המוכר של מספר נגדי ביחס לחיבור.

דוגמה 1.14. המערכת $(\mathbb{Z}, -)$ אינה אפילו חבורה למחצה, מפני שפעולת החיסור אינה קיבוצית. למשל $(5-2)-1 \neq 5-(2-1)$.

הגדרה 1.15. יהי n מספר טבעי. נאמר כי $a, b \in \mathbb{Z}$ הם שקולים בשארית חלוקה ב-n אם $n|a-b$. כלומר קיים $k \in \mathbb{Z}$ כך ש-$a = b+kn$. נסמן זאת $a \equiv b \pmod n$ ונקרא זאת "a שקול ל-b מודולו n".

טענה 1.16. שקילות מודולו n היא יחס שקילות. כפל וחיבור מודולו n מוגדרים היטב. כלומר אם $a \equiv b, c \equiv d \pmod n$, אז $ac \equiv bd \pmod n$ וגם $a+c \equiv b+d \pmod n$.

דוגמה 1.17. נסתכל על אוסף מחלקות השקילות מודולו n, שמקובל לסמן $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[a] : a \in \mathbb{Z}\}$. למשל $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. לפעמים מסמנים את מחלקת השקילות $[a]$ בסימון $\overline{a}$, ולעיתים כאשר ברור ההקשר פשוט a. כזכור $[a]+[b] = [a+b]$ כאשר באגף שמאל הסימן $+$ הוא פעולה בינארית הפועלת על אוסף מחלקות השקילות (a הוא נציג של מחלקת שקילות אחת ו-b הוא נציג של מחלקת שקילות אחרת) ובאגף ימין זו פעולת החיבור הרגילה של מספרים (שלאחריה מסתכלים על מחלקת השקילות שבה $a+b$ נמצא).

אפשר לראות כי $(\mathbb{Z}_n, +)$ היא חבורה אבלית. נבחר נציגים למחלקות השקילות $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$. איבר היחידה הוא $[0]$ (הרי $[0]+[a] = [0+a] = [a]$ לכל $[a]$). קיבוציות הפעולה והאבליות נובעות מהקיבוציות והאבליות של פעולת החיבור הרגילה. האיבר ההופכי של $[a]$ הוא $[n-a]$.

מה ניתן לומר לגבי $(\mathbb{Z}_n, \cdot)$? ישנה סגירות, ישנה קיבוציות וישנו איבר יחידה $[1]$. אך זו לא חבורה כי ל-$[0]$ אין הופכי. נסמן $\mathbb{Z}_n^\circ = \mathbb{Z}_n \setminus \{[0]\}$. האם $(\mathbb{Z}_n^\circ, \cdot)$ חבורה? לא בהכרח. למשל עבור $\mathbb{Z}_6^\circ$ נקבל כי $[2]\,[3] = [6] = [0]$. לפי ההגדרה $[0] \notin \mathbb{Z}_6^\circ$, ולכן הפעולה ב-$(\mathbb{Z}_n^\circ, \cdot)$ אינה בהכרח סגורה (כלומר אפילו לא חבורה למחצה).

דוגמה 1.18. יהי n מספר טבעי. נסמן את הכפולות שלו ב-$n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. למשל $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$. לכל n המערכת $(n\mathbb{Z}, +)$ היא חבורה.

דוגמה 1.19. יהי F שדה (למשל $\mathbb{Q}$, $\mathbb{R}$ או $\mathbb{C}$). אזי $(F, +, 0)$ עם פעולת החיבור של השדה היא חבורה. באופן דומה גם $(M_{n,m}(F), +)$ (אוסף המטריצות בגודל $n \times m$ מעל F) עם פעולת חיבור מטריצות היא חבורה. איבר היחידה הוא מטריצת האפס.

דוגמה 1.20. יהי F שדה. המערכת $(F, \cdot)$ עם פעולת הכפל של השדה היא מונואיד שאינו חבורה (כי 0 לא הפיך). איבר היחידה הוא 1. גם המערכת $(M_n(F), \cdot)$ היא מונואיד ביחס לכפל מטריצות, שכן לא כל מטריצה היא הפיכה.

דוגמה 1.21. יהי F שדה. נסמן $F^* = F \setminus \{0\}$. אזי $(F^*, \cdot, 1)$ היא חבורה. לעומת זאת, המערכת $(\mathbb{Z}^*, \cdot)$ עם הכפל הרגיל של מספרים שלמים היא רק מונואיד (רק $-1, 1$ הפיכים).

הערה 1.22 (אם יש זמן). בקורס באלגברה לינארית כנראה ראיתם הגדרה של שדה $(F, +, \cdot, 0, 1)$ הכוללת רשימה ארוכה של דרישות. בעזרת ההגדרות שראינו נוכל לקצר אותה. נאמר כי F הוא שדה אם $(F, +, 0)$ היא חבורה חילופית, $(F^*, \cdot, 1)$ היא חבורה חילופית וקיום חוק הפילוג (distributive law), לכל $a, b, c \in F$ מתקיים $a(b+c) = ab+ac$).

דוגמה 1.23. קבוצה בעלת איבר אחד ופעולה סגורה היא חבורה. לחבורה זו קוראים החבורה הטריוויאלית.

תרגיל 1.24. האם קיים מונואיד שיש בו איבר הפיך מימין שאינו הפיך משמאל?

פתרון. כן. נבנה מונואיד כזה. תהא X קבוצה. נסתכל על קבוצת ההעתקות מ-X לעצמה המסומנת $X^X = \{f : X \to X\}$. ביחס לפעולת ההרכבה זהו מונואיד, ואיבר היחידה בו הוא העתקת הזהות.

ההפיכים משמאל הם הפונקציות החח"ע. ההפיכים מימין הם הפונקציות על (להזכיר את הטענות הרלוונטיות מבדידה). מה יקרה אם נבחר את X להיות סופית?

אם ניקח למשל $X = \mathbb{N}$ קל למצוא פונקציה על שאינה חח"ע. הפונקציה שנבחר היא $d(n) = \max(1, n-1)$. לפונקציה זו יש הופכי מימין, למשל $u(n) = n + 1$, אבל אין לה הפיך משמאל.

תרגיל 1.25. האם קיימת חבורה למחצה שבה יש איבר יחידה משמאל, אבל אין איבר יחידה מימין?

פתרון. כן, ראיתם את הדוגמה הזו בהרצאה. נתבונן ב-$S = \{\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) : a, b \in \mathbb{R}\}$. קל לראות כי $e' = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ הוא איבר יחידה משמאל.

נראה שאין איבר יחידה מימין. נניח בשלילה שקיים $u = \left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)$ כך שלכל $s \in S$ מתקיים $su = s$. בפרט זה יתקיים עבור $s = \left(\begin{smallmatrix} 1 & b \\ 0 & 0 \end{smallmatrix}\right)$. נקבל כי $su = \left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)$, ולכן $x = 1$ וגם $y = b$. כיון שזה צריך להתקיים לכל $b \in \mathbb{R}$, קיבלנו סתירה לכך ש-u איבר יחידה מימין.

הסבר אחר: נשים לב שישנם אינסוף איברי יחידה משמאל (הם האיברים מהצורה $\left(\begin{smallmatrix} 1 & y \\ 0 & 0 \end{smallmatrix}\right)$), ולכן אין יחידה מימין. כי אם היה איבר יחידה מימין, הוא היה שווה לכל אחד מאיברי היחידה משמאל, אך יש אינסוף איברי יחידה **שונים** משמאל.

תרגיל 1.26 (ממבחן)**.** הוכיחו כי לכל מונואיד $(X, \cdot)$ הקבוצה $P_*(X)$ של כל תתי הקבוצות הלא ריקות של X מגדירה מונואיד ביחס לפעולת הכפל הטבעית:

$$A \bullet B = \{a \cdot b : a \in A, b \in B\}$$

ומצאו מי הם האיברים ההפיכים ב-$(P_*(X), \bullet)$.

פתרון. הקבוצה $P_*(X)$ אינה ריקה, לדוגמה היא מכילה את $\{e\}$ (כאשר e הוא איבר היחידה של X). הפעולה $\bullet$ מוגדרת היטב וסגורה. קל לבדוק כי הפעולה קיבוצית בהתבסס על הקיבוציות של הפעולה ב-X. איבר היחידה ב-$(P_*(X), \bullet)$ הוא $\{e\}$.

האיברים ההפיכים במונואיד הן הקבוצות מהצורה $\{a\}$ עבור a הפיך ב-X (ההופכי הוא $\{a^{-1}\}$). אכן, נניח כי $A \in P_*(X)$ הפיך. לכן קיימת $B \in P_*(X)$ כך שלכל $a \in A, b \in B$ מתקיים $ab = e$. נראה כי $|B| = 1$. אחרת קיימים לפחות שני איברים $b_1, b_2 \in B$ ומתקיים $b_1 a = ab_1 = ab_2 = b_2 a = e$, ולכן מיחידות ההופכי של a נקבל $b_1 = b_2$. באופן סימטרי $|A| = 1$.

הגדרה 1.27 (חבורת האיברים ההפיכים)**.** יהי M מונואיד ויהיו $a, b \in M$ זוג איברים. אם a, b הם הפיכים, אזי גם $a \cdot b$ הוא הפיך במונואיד. אכן, האיבר ההופכי הוא $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. לכן אוסף כל האיברים ההפיכים במונואיד מהווה קבוצה סגורה ביחס לפעולה. כמו כן האוסף הנ"ל מכיל את איבר היחידה, וכל איבר בו הוא הפיך. מסקנה מיידית היא שאוסף האיברים ההפיכים במונואיד מהווה חבורה ביחס לפעולה המצומצמת. נסמן חבורה זו ב-$U(M)$ (קיצור של Units).

הגדרה 1.28. המערכת $(M_n(\mathbb{R}), \cdot)$ של מטריצות ממשיות בגודל $n \times n$ עם כפל מטריצות היא מונואיד. לחבורת ההפיכים שלו

$$U(M_n(\mathbb{R})) = GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$$

קוראים החבורה הלינארית הכללית (ממעלה n) מעל $\mathbb{R}$ (General Linear group).

הגדרה 1.29. נאמר כי פעולה דו־מקומית $* : G \times G \to G$ היא אבלית (או חילופית, commutative) אם לכל שני איברים $a, b \in G$ מתקיים $a * b = b * a$. אם $(G, *)$ חבורה והפעולה היא אבלית, נאמר כי G היא חבורה אבלית (או חילופית). המושג נקרא על שמו של נילס הנריק אָבֶּל (Niels Henrik Abel).

דוגמה 1.30. יהי F שדה. החבורה $(GL_n(F), \cdot)$ אינה אבלית עבור $n > 1$.

דוגמה 1.31. מרחב וקטורי V יחד עם פעולת חיבור וקטורים הרגילה הוא חבורה אבלית.

תרגיל 1.32. תהי G חבורה. הוכיחו שאם לכל $x \in G$ מתקיים $x^2 = 1$, אזי G היא חבורה אבלית.

הוכחה. מן הנתון מתקיים לכל $a, b \in G$ כי $(ab)^2 = a^2 = b^2 = 1$. לכן

$$abab = (ab)^2 = 1 = 1 \cdot 1 = a^2 \cdot b^2 = aabb$$

נכפיל את השיוויון לעיל מצד שמאל בהופכי של a ומצד ימין בהופכי של b, ונקבל $ba = ab$. זה מתקיים לכל זוג איברים, ולכן G חבורה אבלית. □