על שדות

חשבון אינפיניטסימלי (1) - 80131

מרצה: רז קופרמן

מתרגלים: אור יער ודניאל רוזנבלט

סמסטר ב' תשפ"ב, האוניברסיטה העברית

-

אלגברה ליניארית (1) - 80134

מרצה: ערן נבו

מתרגלים: איתמר ישראלי ושני שלומי

סמסטר ב' תשפ"ב, האוניברסיטה העברית

-

סוכם ע"י שריה אנסבכר

תוכן העניינים

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 הגדרה וטענות בסיסיות

תזכורת: פעולה דו-מקומית (בינארית) היא פעולה המקבלת שני איברים (לאו דווקא שונים) ומחזירה אחד, נאמר שפעולה דו-מקומית מוגדרת על קבוצה אם לכל שני איברים בקבוצה תחזיר הפעולה איבר מן הקבוצה.

1.1 הגדרת שדה

הגדרה 1.1. שדה

שדה הוא קבוצה $\mathbb{F}$ בעלת שני איברים שונים (לכל הפחות) הנקראים "אפס" (יסומן ב-0) ו-"אחד" (יסומן ב-1), שעליה מוגדרות שתי פעולות דו-מקומיות הנקראות "חיבור" (תסומן ב-"+") ו-"כפל" (תסומן ב-"$\cdot$"[1]), כך שמתקיימות 9 התכונות הבאות (נקראות גם "אקסיומות השדה"):

תכונה	חיבור (לכל $a,b,c\in\mathbb{F}$)	כפל (לכל $a,b,c\in\mathbb{F}$)
חילוף (קומוטטיביות)	$a+b=b+a$	$a\cdot b=b\cdot a$
קיבוץ (אסוציאטיביות)	$(a+b)+c=a+(b+c)$	$(a\cdot b)\cdot c=a\cdot(b\cdot c)$
קיום איבר אדיש (ניטרלי)	$a+0=a$	$a\cdot 1=a$
קיום איבר נגדי/הופכי	$\exists d\in\mathbb{F}:a+d=0$	$0\neq a\rightarrow\exists d\in\mathbb{F}:a\cdot d=1$
פילוג (דיסטריבוטיביות)	[2]$a\cdot(b+c)=(a\cdot b)+(a\cdot c)$	

♣ נשים לב: החיבור והכפל הן פעולות **דו**-מקומיות, לכן אין דבר כזה חיבור/כפל של שלושה איברים אלא תמיד מחברים/כופלים שניים ואז מחברים/כופלים את התוצאה בשלישי, כלומר המשמעות של $a+b+c$ היא $(a+b)+c$ (קודם מחברים את a ו-b ורק אח"כ מחברים לתוצאה את c).

♣ ניתן להוכיח באינדוקציה שלכל פעולה דו-מקומית המקיימת חילוף וקיבוץ אין שום הבדל אם נסדר את האיברים בצורה כזו או אחרת (ניתן לבצע חילוף גם ליותר משני איברים) וכמו כן אין שום הבדל אם נבצע את הפעולות בסדר כזה או אחר (ניתן לבצע קיבוץ גם ליותר משני איברים), חשוב לשים לב לכך שנדרשים חילוף וקיבוץ יחדיו אך אחד מהם לבדו אינו מספיק.

דוגמה:

$$\begin{aligned}
a+b+c+d: \quad &= \color{red}{((a+b)+c)+d} &&= (a+b)+(c+d) &&= (a+b)+(d+c)\\
&= \color{red}{((a+b)+d)+c} &&= (a+(b+d))+c &&= (a+(d+b))+c\\
&= \color{blue}{((a+d)+b)+c} &&= (a+d)+(b+c) &&= (a+d)+(c+b)\\
&= \color{blue}{((a+d)+c)+b} &&= (a+(d+c))+b &&= (a+(c+d))+b\\
&= \color{green}{((a+c)+d)+b} &&= (a+c)+(d+b) &&= (a+c)+(b+d)\\
&= \color{green}{((a+c)+b)+d}
\end{aligned}$$

אלה שש הדרכים לסדר את החיבור של a,b,c,d כש-a בהתחלה, בעמודה הצבועה ניתן לבצע חילוף בסוגריים הראשונים ולקבל אותיות אחרות בהתחלה ואח"כ לבצע את כל הפעולות הנ"ל כדי לקבל את שאר הדרכים לסדר את החיבור של a,b,c,d.

♣ כשלמדנו ביסודי על חוקי החילוף והקיבוץ שאלתי את עצמי לא פעם מדוע ניתן לבצע את הפעולות ולסדר את האיברים באיזה סדר שנרצה, נכון, זה אמנם אינטואיטיבי מאד אבל לא קיבלנו הסבר מתמטי לזה[3], הפסקה שלעיל היא דוגמה כיצד ניתן להוכיח זאת[4].

[1] פעמים רבות כותבים ab במקום $a\cdot b$, בסיכומים אלו נמעט בכך כדי לשמור על בהירות התוכן.
[2] ישנה מוסכמה שמבצעים כפל לפני חיבור ולכן באגף ימין ניתן היה לכתוב $a\cdot b+a\cdot c$.
[3] שימו לב שההגדרה של כפל וחיבור כפעולות דו-מקומיות היא לא (רק) המצאה של מתמטיקאים שרוצים להניח כמה שפחות ולקבל כמה שיותר, כך אנחנו (או לפחות אני) באמת חושבים על פעולות אלו ולכן יש לשאלה הזו מקום גם בבית-הספר היסודי.
[4] לעומת הטענה בנפנופי ידיים ש-"זה לא משנה באיזה סדר אתה סוכם" אני כן מקבל את אקסיומות השדה כטענות שאינן מצריכות הוכחה (לכן הן נקראות **אקסיומות**), שהרי אין זה משנה מאיזה כיוון נמדוד את אורכם המשותף של שולחנות לאחר שהצמדנו אותם זה לזה.

♣ מאקסיומות השדה נובע שלכל $a,b,c\in\mathbb{F}$ מתקיים גם:

$$\begin{aligned}(a+b)\cdot c=c\cdot(a+b)=c\cdot a+c\cdot b\\1\cdot a=a\\0+a=a\end{aligned}$$

ובנוסף: אם $d\in\mathbb{F}$ הוא נגדי של a אז $d+a=0$ ואם $d\in\mathbb{F}$ הוא הופכי של a (בהנחה ש-$a\neq 0$) אז $d\cdot a=1$.

יהי $\mathbb{F}$ שדה.

1.2 הגדרת חיסור וחילוק

משפט 1.2. יהיו $p,q,r\in\mathbb{F}$ כאשר $p\neq 0$, קיים $x\in\mathbb{F}$ יחיד המקיים $p\cdot x+q=r$.

הוכחה. כדי להוכיח את המשפט נניח שקיים x כזה, נמצא אותו (ובכך נוכיח שאם קיים x כזה אז הוא יחיד) ואח"כ נבדוק אם הוא אכן עונה על הדרישות: יהי $x\in\mathbb{F}$ כך ש-$p\cdot x+q=r$[5],

$$\begin{aligned}&\Rightarrow (p\cdot x+q)+(-q)=r+(-q)\\&\Rightarrow p\cdot x+(q+(-q))=r+(-q)\\&\Rightarrow p\cdot x+0=r+(-q)\\&\Rightarrow p\cdot x=r+(-q)\\&\Rightarrow p^{-1}\cdot(p\cdot x)=p^{-1}\cdot(r+(-q))\\&\Rightarrow \left(p^{-1}\cdot p\right)\cdot x=p^{-1}\cdot(r+(-q))\\&\Rightarrow 1\cdot x=p^{-1}\cdot(r+(-q))\\&\Rightarrow x=p^{-1}\cdot(r+(-q))\end{aligned}$$

מכאן שאם קיים x כזה אז $x=p^{-1}\cdot(r+(-q))$ ואכן אם נגדיר $x:=p^{-1}\cdot(r+(-q))$ נקבל:

$$\begin{aligned}{\color{red}p\cdot x+q}&=p\cdot\left(p^{-1}\cdot(r+(-q))\right)+q\\&=\left(p\cdot p^{-1}\right)\cdot(r+(-q))+q\\&=1\cdot(r+(-q))+q\\&=(r+(-q))+q\\&=r+((-q)+q)\\&=r+0{\color{red}=r}\end{aligned}$$

■

♣ לשיטה שבה השתמשנו בהוכחה קוראים "שיטת ההפיכה"[6] והיא נלמדת כבר בחטיבת הביניים.

♣ בכיתה רז הוכיח קיום (ע"י הגדרת $x:=p^{-1}\cdot(r+(-q))$ והצבתו בביטוי $p\cdot x+r$ כדלעיל) ואח"כ הניח שקיימים $x,y\in\mathbb{F}$ כך ש-$p\cdot x+q=r=q\cdot y+r$ והראה שהדבר גורר את $x=y$.

[5] שימו לב: כשאנחנו כותבים כאן "$-q$" ו-"p^{-1}" אנחנו לא אומרים שיש רק נגדי אחד והופכי אחד (כי עוד לא הוכחנו את זה), אלא שקיימים כאלה ואנחנו לוקחים אחד מהם ומסמנים אותו כך.

[6] המקור היחיד שמצאתי לשם זה הוא הערך "אריאבהטה" (מתמטיקאי הודי) בוויקיפדיה.

מסקנה 1.3. יחידות האיבר האדיש לחיבור

יהיו $a,b\in\mathbb{F}$, אם $a+b=a$ אז $b=0$.

מסקנה 1.4. יחידות הנגדי

יהיו $a,b,c\in\mathbb{F}$, אם $a+b=0$ וגם $a+c=0$ אז $b=c$.

- ♣ בגלל מסקנה זו יש משמעות לסימון $-a$ עבור $a\in\mathbb{F}$.
- ♣ מתקיים $-0=0$.

מסקנה 1.5. יחידות האיבר האדיש לכפל

יהיו $a,x\in\mathbb{F}$ כאשר $a\neq 0$, אם $a\cdot x=a$ אז $x=1$.

מסקנה 1.6. יחידות ההופכי

יהיו $a,b,c\in\mathbb{F}$ כאשר $a\neq 0$, אם $a\cdot b=1$ וגם $a\cdot c=1$ אז $c=b\neq 0$.

- ♣ בגלל מסקנה זו יש משמעות לסימון a^{-1} עבור $0\neq a\in\mathbb{F}$.
- ♣ מתקיים $1^{-1}=1$.

החיסור יוגדר כחיבור הנגדי: לכל $a,b\in\mathbb{F}$ נגדיר $a-b:=a+(-b)$.
החילוק יוגדר ככפל בהופכי: לכל $a,b\in\mathbb{F}$ נגדיר $\frac{a}{b}:=a\cdot b^{-1}$.

- ♣ א"א לחלק ב-0 מפני שלאפס לא יכול להיות הופכי, אם היה הופכי היינו מקבלים סתירה[7]:

$$0=0\cdot 0^{-1}=1$$

בניגוד להגדרת 0 ו-1 כאיברים שונים.

הגדרה 1.7. קבוצה $F\subseteq\mathbb{F}$ תיקרא <u>תת-שדה</u> של $\mathbb{F}$ אם מתקיימים התנאים הבאים:

1. $1\in F$.
2. F סגורה לחיבור: לכל $a,b\in F$ גם $a+b\in F$.
3. F סגורה לכפל: לכל $a,b\in F$ גם $a\cdot b\in F$.
4. F סגורה להופכי: לכל $0\neq a\in F$ גם $a^{-1}\in F$.

1.3 הלימת השוויון לחיבור וכפל

- ♣ במתמטיקה, שוויון בין שני עצמים מציין זהות מוחלטת ביניהם, השוויון הוא יחס המסומן ב-"=" (ניסוח של ויקיפדיה[8]); ישנה הגדרה פורמלית ליחס השוויון אך לא למדנו אותה ולקורס שלנו זה מספיק בהחלט.

ממהותו של השוויון מתקיימים גם:

1. הלימת השוויון לחיבור - לכל $a,b,c\in\mathbb{F}$ כך ש-$a=b$ מתקיים $a+c=b+c$, מחוק החילוף לחיבור נסיק שגם $c+a=c+b$.
2. הלימת השוויון לכפל - לכל $a,b,c\in\mathbb{F}$ כך ש-$a=b$ מתקיים $a\cdot c=b\cdot c$, מחוק החילוף לכפל נסיק שגם $c\cdot a=c\cdot b$.

[7] בהמשך נוכיח שלכל $a\in\mathbb{F}$ מתקיים $0\cdot a=a\cdot 0=0$.
[8] ראו ערך "שוויון (מתמטיקה)".

1.4 דוגמאות

♣ הדוגמאות הכי מוכרות לשדות הם: שדה המספרים הרציונליים ($\mathbb{Q}$), שדה המספרים הממשיים ($\mathbb{R}$) ושדה המספרים המרוכבים ($\mathbb{C}$); $\mathbb{Q}$ הוא תת-שדה של $\mathbb{R}$ ו-$\mathbb{R}$ הוא תת-שדה של $\mathbb{C}$.
את שני השדות הראשונים ($\mathbb{Q}$ ו-$\mathbb{R}$) אנחנו נגדיר היטב כשנעסוק במספרים הממשיים באינפי' 1, ועל שדה המרוכבים ($\mathbb{C}$) כתבתי באריכות בקובץ "המספרים המרוכבים".

2 טענות נוספות

2.1 התחלה

משפט 2.1. חוקי הצמצום
יהיו $a,b,c\in\mathbb{F}$,

- אם $a+b=a+c$ אז $b=c$, מחוק החילוף לחיבור נסיק גם שאם $b+a=c+a$ אז $b=c$.
- נניח ש-$a\neq 0$, אם $a\cdot b=a\cdot c$ אז $b=c$, מחוק החילוף לכפל נסיק גם שאם $b\cdot a=c\cdot a$ אז $b=c$.

משפט 2.2. לכל $a\in\mathbb{F}$ מתקיים $0\cdot a=a\cdot 0=0$.

הוכחה. יהי $a\in\mathbb{F}$.

$$\begin{aligned}
&\Rightarrow a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0\\
&\Rightarrow a\cdot 0+(-(a\cdot 0))=(a\cdot 0+a\cdot 0)+(-(a\cdot 0))\\
&\Rightarrow 0=a\cdot 0+(a\cdot 0+(-(a\cdot 0)))\\
&\Rightarrow 0=a\cdot 0+0\\
&\Rightarrow 0=a\cdot 0
\end{aligned}$$

■

משפט 2.3. יהיו $a,b\in\mathbb{F}$, מתקיים $a\cdot b=0$ אם"ם $a=0$ ו/או $b=0$.

הוכחה.

- $\Rightarrow$

  נובע ישירות מהמשפט הקודם (2.2).

- $\Leftarrow$

  נניח ש-$a\cdot b=0$ ובנוסף $a\neq 0$ (מכאן שיש ל-a הופכי).

$$\begin{aligned}
&\Rightarrow a^{-1}\cdot(a\cdot b)=a\cdot 0\\
&\Rightarrow \left(a^{-1}\cdot a\right)\cdot b=0\\
&\Rightarrow 1\cdot b=0\\
&\Rightarrow b=0
\end{aligned}$$

  א"כ לא ייתכן ש-$a\neq 0$ וגם $b\neq 0$ כלומר $a=0$ ו/או $b=0$.

■

טענה 2.4. לכל $a,b\in\mathbb{F}$ מתקיימים כל הפסוקים הבאים:

1. אם $a\neq 0$ אז $a^{-1}\neq 0$.
2. $-(-a)=a$.
3. אם $a\neq 0$ אז $\left(a^{-1}\right)^{-1}=a$.
4. $(-1)\cdot a=-a$.
5. $a\neq 0$ אמ"ם $-a\neq 0$.
6. $a=b$ אמ"ם $a-b=0$.
7. $-(a+b)=-a-b$.
8. $-(a-b)=b-a$.
9. $(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$.
10. $(-a)\cdot(-b)=a\cdot b$.

הוכחה.

- סעיף 1 נובע ממשפט 2.3 ומהעובדה ש-$a\cdot a^{-1}=1\neq 0$.
- כדי להוכיח את סעיפים 2-5 יש להשתמש ביחידות הנגדי וההופכי.
- בסעיף 6 נוסיף b לשני האגפים כדי להוכיח את הגרירה משמאל לימין, ובשביל הגרירה ההפוכה נוסיף לשני האגפים את $-b$.
- כדי להוכיח את סעיפים 7-8 ניתן להשתמש ביחידות הנגדי או בסעיף 4.
- סעיפים 9-10 נובעים מסעיף 4.

■

טענה 2.5. לכל $a,b,c,d\in\mathbb{F}$, מתקיימים כל הפסוקים הבאים:

1. אם $a,b\neq 0$ אז $(a\cdot b)^{-1}=a^{-1}\cdot b^{-1}$
2. אם $a\neq 0$ אז $\frac{0}{a}=0$
3. $\frac{a}{1}=a$
4. אם $b,d\neq 0$ אז $\frac{a}{b}=\frac{c}{d}$ אם"ם $a\cdot d=b\cdot c$
5. אם $b,d\neq 0$ אז $\left(\frac{b}{d}\right)^{-1}=\frac{d}{b}$
6. אם $b,d\neq 0$ אז $\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}$
7. אם $b,d\neq 0$ אז $\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+b\cdot c}{b\cdot d}$

הוכחה.

1. נובע מיחידות ההופכי.
2. נובע ממשפט 2.2 ומסעיף 1 בטענה 2.4.
3. נובע מהשוויון $1^{-1}=1$ (שנובע מיחידות ההופכי).
4. נובע מאריתמטיקה פשוטה[9].
5. נובע מיחידות ההופכי.
6. נובע מחילוף וקיבוץ של כפל.
7.

$$\begin{aligned}
\frac{a}{b}+\frac{c}{d} &= a\cdot b^{-1}+c\cdot d^{-1}\\
&= \left(a\cdot b^{-1}\right)\cdot 1+\left(c\cdot d^{-1}\right)\cdot 1\\
&= \left(a\cdot b^{-1}\right)\cdot\left(d\cdot d^{-1}\right)+\left(c\cdot d^{-1}\right)\cdot\left(b\cdot b^{-1}\right)\\
&= a\cdot\left(b^{-1}\cdot\left(d\cdot d^{-1}\right)\right)+c\cdot\left(d^{-1}\cdot\left(b\cdot b^{-1}\right)\right)\\
&= a\cdot\left(\left(b^{-1}\cdot d\right)\cdot d^{-1}\right)+c\cdot\left(\left(d^{-1}\cdot b\right)\cdot b^{-1}\right)\\
&= a\cdot\left(\left(d\cdot b^{-1}\right)\cdot d^{-1}\right)+c\cdot\left(\left(b\cdot d^{-1}\right)\cdot b^{-1}\right)\\
&= a\cdot\left(d\cdot\left(b^{-1}\cdot d^{-1}\right)\right)+c\cdot\left(b\cdot\left(d^{-1}\cdot b^{-1}\right)\right)\\
&= (a\cdot d)\cdot\left(b^{-1}\cdot d^{-1}\right)+(c\cdot b)\cdot\left(b^{-1}\cdot d^{-1}\right)\\
&= ((a\cdot d)+(c\cdot b))\cdot\left(b^{-1}\cdot d^{-1}\right)\\
&= \frac{a\cdot d+b\cdot c}{b\cdot d}
\end{aligned}$$

■

[9] נכפול את שני האגפים ב-$b\cdot d$ כדי להוכיח את הגרירה מימין לשמאל וב-$b^{-1}\cdot a^{-1}$ כדי להוכיח את הגרירה ההפוכה.

משפט 2.6. נוסחאות הכפל המקוצר
לכל $a,b\in\mathbb{F}$ מתקיים:

1. $(a\pm b)\cdot(a\pm b)=a\cdot a\pm(1+1)\cdot a\cdot b+b\cdot b$
2. $(a+b)\cdot(a-b)=a\cdot a-b\cdot b$

הוכחה. מתקיים:

.1

$$\begin{aligned}
(a\pm b)\cdot(a\pm b) &= (a\pm b)\cdot a+(a\pm b)\cdot(\pm b)\\
&= [a\cdot a+(\pm b)\cdot a]+[a\cdot(\pm b)+(\pm b)\cdot(\pm b)]\\
&= [a\cdot a+(\pm b)\cdot a]+[(\pm b)\cdot a+b\cdot b]\\
&= ([a\cdot a+(\pm b)\cdot a]+(\pm b)\cdot a)+b\cdot b\\
&= (a\cdot a+[(\pm b)\cdot a+(\pm b)\cdot a])+b\cdot b\\
&= [a\cdot a+([(\pm 1)\cdot b]\cdot a+[(\pm 1)\cdot b]\cdot a)]+b\cdot b\\
&= [a\cdot a+((\pm 1)\cdot[b\cdot a]+(\pm 1)\cdot[b\cdot a])]+b\cdot b\\
&= [a\cdot a+(\pm 1\pm 1)\cdot(b\cdot a)]+b\cdot b\\
&= [a\cdot a\pm(1+1)\cdot(b\cdot a)]+b\cdot b\\
&= [a\cdot a\pm(1+1)\cdot(a\cdot b)]+b\cdot b\\
&= a\cdot a\pm(1+1)\cdot a\cdot b+b\cdot b
\end{aligned}$$

.2

$$\begin{aligned}
(a+b)\cdot(a-b) &= (a+b)\cdot a+(a+b)\cdot(-b)\\
&= (a+b)\cdot a+(-b)\cdot(a+b)\\
&= (a+b)\cdot a+[(-1)\cdot b]\cdot(a+b)\\
&= (a+b)\cdot a+(-1)\cdot[b\cdot(a+b)]\\
&= (a+b)\cdot a-[b\cdot(a+b)]\\
&= (a\cdot a+b\cdot a)-(b\cdot a+b\cdot b)\\
&= (a\cdot a+b\cdot a)+(-b\cdot a-b\cdot b)\\
&= [(a\cdot a+b\cdot a)-b\cdot a]-b\cdot b\\
&= [a\cdot a+(b\cdot a-b\cdot a)]-b\cdot b\\
&= [a\cdot a+0]-b\cdot b\\
&= a\cdot a-b\cdot b
\end{aligned}$$

■

מסקנה 2.7. יהיו $a,b\in\mathbb{F}$ מתקיים: $a\cdot a=b\cdot b$ אם"ם $a=b$ ו/או ש-$a=-b$, בפרט מתקיים: $a\cdot a=1\cdot 1=1$ אם"ם $a=1$ ו/או ש-$a=-1$.

הוכחה. יהיו $a,b\in\mathbb{F}$, הגרירה משמאל לימין נובעות מסעיף 10 בטענה 2.4.
כדי להוכיח את הגרירות מימין לשמאל נשים לב לכך שמנוסחת הכפל המקוצר השנייה נובע כי:

$$(a+b)\cdot(a-b)=a\cdot a-b\cdot b=0$$

ולכן ממשפט 2.3 נובע ש-$a+b=0$ ו/או $a-b=0$ ומכאן ש-$a=-b$ ו/או $a=b$. ■

2.2 האם סיימנו? ממש לא!

♣ בשלב זה ניתן אולי להשתכנע שכל התכונות של המספרים שאנחנו מכירים נובעות מאקסיומות השדה אך המצב שונה בתכלית, לדוגמה: אנחנו יודעים שעבור שני מספרים a ו-b השוויון $a-b=b-a$ גורר ש-$a=b$ אך האם ניתן להוכיח זאת ע"י אקסיומות השדה? ננסה ונראה: יהיו $a,b\in\mathbb{F}$ כך ש-$a-b=b-a$,

$$\begin{aligned}
&\Rightarrow (a+(-b))+(b+a)=(b+(-a))+(b+a)\\
&\Rightarrow (a+(-b))+(b+a)=(b+(-a))+(a+b)\\
&\Rightarrow ((a+(-b))+b)+a=((b+(-a))+a)+b\\
&\Rightarrow ((a+(-b))+b)+a=((b+(-a))+a)+b\\
&\Rightarrow (a+(-b+b))+a=(b+((-a)+a))+b\\
&\Rightarrow (a+0)+a=(b+0)+b\\
&\Rightarrow a+a=b+b\\
&\Rightarrow a\cdot 1+a\cdot 1=b\cdot 1+b\cdot 1\\
&\Rightarrow a\cdot(1+1)=b\cdot(1+1)
\end{aligned}$$

כעת אם היינו יודעים ש-$1+1\neq 0$ היינו יכולים לכפול ב-$(1+1)^{-1}$ מימין ולקבל $a=b$ כנדרש אך כפי שנראה מיד קיימים שדות שבהם $1+1=0$ ולכן א"א להשלים את ההוכחה בהתבסס על אקסיומות השדה בלבד.

דוגמה 2.8. נגדיר $\mathbb{F}_2:=\{0,1\}$ עם פעולות החיבור והכפל הבאות:

$\cdot$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

הקבוצה $\mathbb{F}_2$ והפעולות "+" ו-"·" מקיימות את כל התנאים ולכן $\mathbb{F}_2$ (יחד עם הפעולות הנ"ל) הוא שדה.
סימנו באדום את מה שאינו תוצאה ישירה של הגדרת השדה.

♣ ב-$\mathbb{F}_2$ אכן מתקיים $0-1=-1=1=1-0$ למרות ש-$1\neq 0$.

2.3 דוגמאות נוספות

דוגמה 2.9. $\mathbb{F}_2$ שייך למשפחה של שדות המסומנים ב-$\mathbb{F}_p$ כאשר p ראשוני:
יהי $p\in\mathbb{N}$ מספר ראשוני ונסמן $\mathbb{F}_p:=\{0,1,\ldots,p-1\}$, פעולות החיבור והכפל של $\mathbb{F}_p$ יוגדרו ע"י פעולות החיבור והכפל בשלמים מודולו p - כלומר נחבר/נכפול את המספרים ב-$\mathbb{Z}$ וניקח את השארית של חלוקת התוצאה ב-p; לדוגמה ב-$\mathbb{F}_7$ מתקיים $3\cdot 5=15=1$ ו-$3+5=8=1$ כי 1 הוא השארית של חילוק 15 ו-8 ב-7.

- ♣ בעצם מה שקורה ב-$\mathbb{F}_2$ הוא כזה: אם ב-$\mathbb{Z}$ המספר זוגי אז הוא שווה ל-0 ואם הוא אי-זוגי אז הוא שווה ל-1, זו הסיבה לדמיון בין טבלאות החיבור והכפל שלעיל לבין הכללים:

1. זוגי ועוד זוגי שווה זוגי.
2. זוגי ועוד אי-זוגי שווה אי-זוגי.
3. זוגי כפול כל מספר שווה זוגי.
4. אי-זוגי כפול אי-זוגי שווה אי-זוגי.

- ♣ א"כ שני איברים ב-$\mathbb{Z}$ יחשבו שווים זה לזה ב-$\mathbb{F}_p$ אם השאריות שלהם בחלוקה ב-p שוות.

- ♣ כל התכונות של $\mathbb{F}_p$ כשדה מתקבלות מהעובדה שתכונות אלו מאפיינות גם את השלמים[10] מלבד אחת: הקיום של מספר הופכי (ב-$\mathbb{Z}$ קיימים מספרים שונים מ-0 שאין להם איבר הופכי), לכן עלינו להוכיח אותה בפירוש:

הוכחה. יהי $0\neq a\in\mathbb{F}_p$ ונתבונן בקבוצה $\{1\cdot a,2\cdot a,\ldots,(p-1)\cdot a\}$, אף אחד מן המספרים בקבוצה אינו מתחלק ב-p ראשוני ובכל איבר אינו מחלק אף אחד משני המוכפלים, מכאן שאם הקבוצה הנ"ל בגודל $p-1$ (כלומר אין בהצגתה חזרה על אותו איבר פעמיים) אז קיים $p>b\in\mathbb{N}$ כך ש-$a\cdot b=1$ ב-$\mathbb{F}_p$.
נוכיח שזהו אכן המצב: יהיו $c,b\in\mathbb{F}_p$ כך ש-$b\cdot a=c\cdot a$, מכאן ש-$(b-c)\cdot a=0$ ב-$\mathbb{F}_p$, כלומר המספר $(b-c)\cdot a$ מתחלק ב-p כשהוא ב-$\mathbb{Z}$; אנחנו יודעים ש-p אינו מחלק את a ולכן נובע מזה ש-p מחלק את $b-c$, כלומר השארית של חלוקת b ב-p שווה לשארית של חלוקת c ב-p ולכן ב-$\mathbb{F}_p$ מתקיים $b=c$, א"כ אין בקבוצה הנ"ל חזרות. ■

- ♣ בניגוד ל-$\mathbb{Q}$, $\mathbb{R}$ ו-$\mathbb{C}$ שדה מהצורה $\mathbb{F}_p$ הוא <u>שדה סופי</u>.

- ♣ <u>המאפיין</u> (נקרא גם <u>המציין</u> או <u>הקרקטריסטיקה</u>) של שדה הוא המספר הראשון בסדרה:

$$1,1+1,1+1+1,1+1+1+1\ldots$$

ששווה ל-0 בשדה (כלומר זהו המספר הטבעי הקטן ביותר ששווה לאפס בשדה), עבור שדות שבהם אף אחד מן המספרים הללו אינו אפס אומרים שהמאפיין של השדה הוא 0.

[10] אם שני מספרים שווים זה לזה ב-$\mathbb{Z}$ ודאי שהם משאירים את אותה שארית בחלוקה ב-p ולכן הם שווים גם ב-$\mathbb{F}_p$.