תורת החוגים - הגדרות 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:
אקסיומות השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 חוגים כלליים

1.1 התחלה

הגדרה 1.1. חוג

חוג הוא קבוצה R בעלת איברים 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 7 התכונות הבאות:

תכונה	חיבור (לכל $a,b,c\in R$)	כפל (לכל $a,b,c\in R$)
חילוף (קומוטטיביות)	$a+b=b+a$	-
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	$\exists d\in R: a+d=0$	-
פילוג (דיסטריבוטיביות)	[2] $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ [3] $(b+c)\cdot a=(b\cdot a)+(c\cdot a)$	

במילים אחרות חוג הוא קבוצה R, איברים מיוחדים "0" ו-"1" ושתי פעולות "+" ו-"$-$" כך ש-$(R,+,0)$ היא חבורה אבלית, ובנוסף הכפל אסוציאטיבי ובעל איבר יחידה.

- ♣ מבחינה פורמלית חוג הוא סדרה בעלת חמישה איברים $(R,+,\cdot,0,1)$.
- ♣ בניגוד לשדה בו $0\neq 1$, בחוג איננו דורשים זאת, ואכן הקבוצה $\{0\}$ היא חוג (נקרא החוג הטריוויאלי).
- ♣ לעתים מגדירים חוג ללא הקיום של איבר אדיש לכפל, ואז קוראים לחוגים שהגדרנו כאן "חוגים עם יחידה" (ובהתאמה חוגים שאינם כאלה נקראים גם "חוגים בלי יחידה"). אנחנו לא נעשה זאת בקורס זה, כל חוג שנדבר עליו יהיה חוג עם יחידה אלא אם נאמר אחרת במפורש.

רשימת חוגים שאנחנו כבר מכירים

1. שדות: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ והשדות מהצורה $\mathbb{F}_p$ עבור p ראשוני.
2. חוג השלמים $\mathbb{Z}$.
3. חוג הפולינומים $\mathbb{F}[x]$ מעל שדה $\mathbb{F}$.
4. החוג המודולרי $\mathbb{Z}_n$ - לכל שני מספרים שלמים בקבוצה $\{0,1,\ldots,n-1\}$ נגדיר את פעולות החיבור והכפל ע"י החיבור ב-$\mathbb{Z}$, וכדי שנקבל איבר בקבוצה נחלק ב-n עם שארית וניקח את השארית; ראינו בליניארית 1 שאם n ראשוני אז $\mathbb{Z}_n$ הוא שדה.
5. מרחב המטריצות $M_n(\mathbb{F})$ מעל שדה $\mathbb{F}$ עם פעולות החיבור וכפל מטריצות (דוגמה זו היא הדוגמה היחידה ברשימה לחוג שאינו חילופי), ובהתאמה עבור מ"ו נ"ס V גם $\operatorname{End}(V)$ (שהוא מרחב ההעתקות הליניאריות מ-V לעצמו) הוא חוג ביחס לחיבור העתקות ליניאריות והרכבתן.

הגדרה 1.2. חוג R ייקרא חוג חילוק אם לכל $0\neq r\in R$ קיים $s\in R$ כך ש-$r\cdot s=1=s\cdot r$.

---

[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] ראה הערה קודמת.

יהי R חוג.

סימון: נסמן $R^* := R^\times := \{a \in R \mid \exists x \in R\ a \cdot x = 1\}$, כלומר $R^\times$ היא קבוצת האיברים ב-R שיש להם הופכי ימני[4].

מסקנה 1.3. $R^\times$ היא חבורה ביחס לכפל של R; חבורה זו נקראת החבורה הכפלית[5] של R (או חבורת היחידות של R).

♣ איבר היחידה הוא 1 וההופכי הוא ההופכי השמאלי, כלומר אנו טוענים ש-1 הוא גם איבר יחידה ימני עבור האיברים ב-$R^\times$ וההופכי השמאלי הוא גם הופכי ימני).

♣ ראינו את הטענה הזו בקורס הקודם (הטענה השנייה בקובצי הטענות וההוכחות).

הגדרה 1.4. תת-חוג

תת-קבוצה $S \subseteq R$ תיקרא תת-חוג של R אם היא סגורה לחיבור, לכפל ולנגדי[6], ובנוסף $1_R \in S$; במקרה כזה נסמן $S \leqslant R$.

מסקנה 1.5. כל תת-חוג של R הוא חוג בפני עצמו ביחס לאותן פעולות חיבור וכפל ואותם איברים אדישים.

1.2 אידיאלים

הגדרה 1.6. אידיאל

- תת-קבוצה $I \subseteq R$ תיקרא אידיאל שמאלי של R אם לכל $a, b \in I$ מתקיימים שלושת התנאים הבאים:
  1. $0 \in I$ (כמו תמיד, ניתן להחליף תנאי זה בכך ש-$I \neq \emptyset$).
  2. לכל $a, b \in I$ מתקיים $a + b \in I$.
  3. לכל $a \in I$ ולכל $r \in R$ מתקיים $r \cdot a$.
- תת-קבוצה $I \subseteq R$ תיקרא אידיאל ימני של R אם לכל $a, b \in I$ מתקיימים שלושת התנאים הבאים:
  1. $0 \in I$ (כמו תמיד, ניתן להחליף תנאי זה בכך ש-$I \neq \emptyset$).
  2. לכל $a, b \in I$ מתקיים $a + b \in I$.
  3. לכל $a \in I$ ולכל $r \in R$ מתקיים $a \cdot r$.
- תת-קבוצה $I \subseteq R$ תיקרא אידיאל דו-צדדי (או סתם אידיאל) אם היא אידיאל שמאלי וגם אידיאל ימני.

♣ במילים אחרות תת-קבוצה $I \subseteq R$ תיקרא אידאל שמאלי/ימני של R אם $(I, +, 0)$ היא תת-חבורה של R ובנוסף לכל $a \in I$ ולכל $r \in R$ מתקיים $r \cdot a$ או $a \cdot r$ (בהתאמה).

סימון: אם תת-קבוצה $I \subseteq R$ היא אכן אידיאל נסמן זאת ע"י $I \trianglelefteq R$ או ב-$I \triangleleft R$.

♣ זה לא מיקרי שהסימון של אידיאל הוא אותו סימון של תת-חבורה נורמלית, אנחנו נראה שיש בין שני המושגים דמיון רב.

האידיאלים שנדבר עליהם מכאן ואילך הם אידיאלים דו-צדדיים.

הגדרה 1.7. אידיאל $I \trianglelefteq R$ ייקרא טריוויאלי אם $I = R$ ו/או $I = \{0\}$.

הגדרה 1.8. נאמר ש-R הוא חוג פשוט אם $R \neq \{0\}$ והאידיאלים היחידים של R הם הטריוויאליים.

הגדרה 1.9. אידיאל $I \trianglelefteq R$ ייקרא מקסימלי אם $I \neq R$ והאידיאלים היחידים של R המכילים את I הם R ו-I.

[4] הדרישה שההופכי יהיה ימני היא מפני שהגדרנו גם את 1 בתור איבר יחידה ימני, ורק במקרה כזה המסקנה הבאה תהיה תקפה.

[5] להבדיל מהחבורה החיבורית שהיא החוג כולו ביחס לפעולת החיבור.

[6] לכל $a \in S$ גם $-a \in S$.

לא ברור לי אם בקורס שלנו דורשים את התנאי ש-$I \neq R$ כדי שיהיה מקסימלי או ש-R כן נחשב מקסימלי.

טענה. 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.

הגדרה 1.10. תהא $S \subseteq R$ תת-קבוצה, האידיאל הנוצר ע"י S (מסומן ע"י (S)) הוא חיתוך כל האידיאלים המכילים את S.

מסקנה 1.11. תהא $S \subseteq R$ תת-קבוצה, מתקיימים שלושת הפסוקים הבאים:

1. (S) הוא אידיאל של R.
2. $S \subseteq (S)$.
3. לכל אידיאל $I \trianglelefteq R$ המכיל את S מתקיים $(S) \subseteq I$.

הגדרה 1.12. יהי $I \trianglelefteq R$ אידיאל, נאמר שתת-קבוצה $S \subseteq I$ היא קבוצת יוצרים של I אם $I = (S)$.

סימון: עבור קבוצה סופית $\{s_1, s_2, \ldots, s_n\} \subseteq R$ נכתוב גם $(s_1, s_2, \ldots, s_n) := (\{s_1, s_2, \ldots, s_n\})$.

הגדרה 1.13. נאמר שאידיאל $I \trianglelefteq R$ נוצר סופית אם הוא נוצר ע"י קבוצה סופית $S \subseteq R$, וכמו כן נאמר שאידיאל $I \trianglelefteq R$ הוא אידיאל ראשי אם קיים $a \in R$ כך ש-$I = (a)$.

למה 1.14. יהי $I \trianglelefteq R$ אידיאל, I הוא תת-חבורה נורמלית של $(R, +, 0)$ ולכן מוגדרת על חבורת המנה R/I פעולת חיבור. נגדיר על R/I פעולת כפל ע"י (לכל $a, b \in R$):

$$(a+I) \cdot (b+I) := a \cdot b + I$$

פעולה זו אכן מוגדרת היטב, ו-$(R/I, +, \cdot, I, 1+I)$ הוא חוג.

♣ בעוד שאכן מתקיים $(a+b+I) = \{a+b+i \mid i \in I\} = \{a+i+b+j \mid i,j \in I\}$,
מתקיים רק $a \cdot b + I \subseteq \{a \cdot b + aI + bI + I \mid i,j \in I\} = \{(a+i)(b+j) \mid i,j \in I\}$.

הגדרה 1.15. לכל אידיאל $I \trianglelefteq R$ נקרא לחוג שבלמה הקודמת (1.14) חוג המנה של I.

2 הומומורפיזמים

יהיו R ו-S חוגים.

הגדרה 2.1. הומומורפיזם

פונקציה $\varphi : R \to S$ תיקרא הומומורפיזם (של חוגים) אם היא מקיימת את שלושת התנאים הבאים:

1. לכל $a, b \in R$ מתקיים $\varphi(a+b) = \varphi(a) + \varphi(b)$.
2. לכל $a, b \in R$ מתקיים $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.
3. מתקיים $\varphi(1_R) = 1_S$.

♣ התנאי השלישי אינו נובע משני האחרים - העתקת האפס מקיימת את שני הראשונים אך אינה מקיימת אותו.

הגדרה 2.2. יהי $\varphi : R \to S$ הומומורפיזם.

- נאמר ש-φ הוא מונומורפיזם (או שיכון) אם הוא חח"ע, ובמקרה כזה נסמן גם $\varphi : R \hookrightarrow S$.
- נאמר ש-φ הוא אפימורפיזם (ביחס ל-S[7]) אם הוא על, ובמקרה כזה נסמן גם $\varphi : R \twoheadrightarrow S$.
- נאמר ש-φ הוא איזומורפיזם (ביחס ל-S) אם הוא חח"ע ועל[8], ובמקרה כזה נסמן גם $\varphi : R \xrightarrow{\sim} S$.
- נאמר ש-φ הוא אנדומורפיזם אם $R = S$, קבוצת האנדומורפיזמים של R מסומנת ב-$\mathrm{End}(R)$.
- נאמר ש-φ הוא אוטומורפיזם אם הוא חח"ע ועל ובנוסף $R = S$[9], קבוצת האוטומורפיזמים של R מסומנת ב-$\mathrm{Aut}(R)$.

הגדרה 2.3. יהי $\varphi : R \to S$ הומומורפיזם, הגרעין של φ הוא הקבוצה:

$$\ker\varphi := \{r \in R : \varphi(r) = 0_S\}$$

טענה 2.4. הפונקציה ההופכית של איזומורפיזם גם היא איזומורפיזם.

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

הגדרה 2.5. נאמר ש-R ו-S איזומורפיים זה לזה אם קיים איזומורפיזם $\varphi : R \to S$, ובמקרה כזה נסמן $R \cong S$ (איזומורפיות הוא יחס שקילות).

[7] אנחנו נראה בקובץ הטענות שהתמונה של כל הומומורפיזם היא תת-חוג של הטווח ולכן φ הוא אפימורפיזם ביחס ל-$\mathrm{Im}\varphi$.
[8] כלומר φ הוא מונורמפיזם ואפימורפיזם.
[9] כלומר אם φ הוא איזומורפיזם ואנדומורפיזם.

3 חוגים חילופיים (קומוטטיביים)

הגדרה 3.1. חוג חילופי

חוג R ייקרא חוג חילופי (או קומוטטיבי) אם בנוסף להיותו חוג הכפל שלו מקיים את חוק החילוף (קומוטטיבי), כלומר לכל $a,b\in R$ מתקיים $a\cdot b=b\cdot a$.

- ♣ בחוג חילופי כל אידיאל שמאלי/ימני הוא אידיאל דו-צדדי.
- ♣ מבין כל החוגים שראינו עד כה רק חוג המטריצות אינו חוג חילופי.

הגדרה 3.2. המֶרְכָּז

המרכז של חוג R הוא הקבוצה $Z\left(R\right):=\left\{z\in R\mid\forall r\in R\ rz=zr\right\}$.

מסקנה 3.3. המרכז של כל חוג הוא תת-חוג חילופי.

יהי R חוג חילופי שאינו טריוויאלי.

3.1 יחס החלוקה

הגדרה 3.4. יהיו $a,b\in R$, נאמר ש-a מחלק את b, ונסמן $a\mid b$, אם קיים $q\in R$ כך ש-$b=a\cdot q$.

הגדרה 3.5. יהיו $a,b\in R$, נאמר ש-a ו-b הם ידידים (או חברים), ונסמן $a\sim b$ אם $a\mid b$ וגם $b\mid a$.

מסקנה 3.6. חברות הוא יחס שקילות.

הגדרה 3.7. איבר $0\neq r\in R$ שאינו הפיך ייקרא אי-פריק אם לכל $a,b\in R$ כך ש-$r=a\cdot b$, r ו-a ידידים ו/או ש-r ו-b ידידים, אחרת ייקרא פריק.

הגדרה 3.8. איבר $0\neq p\in R$ שאינו הפיך ייקרא ראשוני אם לכל $a,b\in R$ כך ש-$p=a\cdot b$ מתקיים $p\mid a$ ו/או $p\mid b$.

הגדרה 3.9. אידיאל $I\trianglelefteq R$ ייקרא אידיאל ראשוני אם $I\neq R$ ולכל $a,b\in R$ כך ש-$a\cdot b\in I$ מתקיים $a\in I$ ו/או $b\in I$.

מסקנה 3.10. לכל איבר $0\neq p\in R$ שאינו הפיך מתקיים: p ראשוני אם"ם (p) הוא אידיאל ראשוני.

הגדרה 3.11. יהיו $a_1,a_2,\ldots,a_n\in R$ שלפחות אחד מהם שונה מ-0, איבר $d\in R$ ייקרא מחלק משותף מקסימלי (ובקיצור ממ"מ או gcd) של $a_1,a_2,\ldots,a_n$ אם הוא מקיים את שני התנאים הבאים:

1. $d\mid a_i$ לכל $n\geq i\in\mathbb{N}$ (כלומר d הוא מחלק משותף).
2. לכל $\tilde{d}\in\mathbb{R}$ כך ש-$\tilde{d}\mid a_i$ לכל $n\geq i\in\mathbb{N}$, מתקיים $\tilde{d}\mid d$.

- ♣ נוהגים לסמן מחלק משותף מקסימלי ב-$\gcd\left(a_1,a_2,\ldots,a_n\right)$ או ב-$\left(a_1,a_2,\ldots,a_n\right)$, אבל בניגוד לחוג השלמים שבו קיימים בדיוק שני מחלקים משותפים מקסימליים ואנו בוחרים את החיובי מביניהם, בחוגים כלליים אין דרך לבחור באופן קנוני אחד מהמחלקים המשותפים המקסימליים ולכן סימון זה אינו מוגדר; עם זאת, כפי שאמרנו נוהגים לכתוב כך אך יש לשים לב לכך שלא מודבר באיבר קבוע.
- ♣ בחוגים כלליים ייתכן שקיימים איברים שעבורם אין מחלק משותף מקסימלי.

מסקנה 3.12. לכל $a_1,a_2,\ldots,a_n\in R$ שלפחות אחד מהם שונה מ-0, כל שני מחלקים משותפים מקסימליים של $a_1,a_2,\ldots,a_n$ הם ידידים.

מה עם כפולה משותפת מינימלית?

3.2 תחומי שלמות

הגדרה 3.13. נאמר שאיבר $0 \neq a \in R$ הוא מחלק אפס אם קיים $0 \neq b \in R$ כך ש-$a \cdot b = 0$.

הגדרה 3.14. תחום שלמות
נאמר ש-R הוא תחום שלמות אם אין בו מחלקי אפס, כלומר לכל $a, b \in R$ כך ש-$a \cdot b = 0$ מתקיים $a = 0$ ו/או $b = 0$.

♣ מבין כל החוגים החילופיים שראינו עד כה רק החוג המודולרי $\mathbb{Z}_n$ אינו תחום שלמות (כאשר n אינו 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[10]:

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

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

הגדרה 3.15 Q ייקרא שדה השברים של R.

♣ כמובן שההשראה להגדרה זו הגיעה מהבנייה של שדה המספרים הרציונליים מתוך חוג השלמים.

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

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

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

הגדרה 3.16. שדה השברים של $\mathbb{F}[x]$ ייקרא שדה הפונקציות הרציונליות.

♣ למרות השם לא מדובר בפונקציות ממש - נזכור ששני פולינומים יכולים להיות שונים למרות שהפונקציות שהם מגדירים שוות.

---

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

3.3 תחומי פריקות חד-ערכית

הגדרה 3.17. R[11] ייקרא תחום פריקות חד-ערכית (או בקיצור תחום פח"ע) אם לכל איבר $0 \neq r \in R$ שאינו הפיך קיימים $p_1, p_2, \ldots, p_n \in R$ אי-פריקים יחידים (עד כדי שינוי סדר וחברות), אך לאו דווקא שונים זה מזה, כך שמתקיים:

$$r = \prod_{i=1}^{n} p_i$$

כלומר אם גם $q_1, q_2, \ldots, q_s \in R$ הם אי-פריקים המקיימים $r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ אז קיימת פונקציה חח"ע ועל $f : \{i \in \mathbb{N} \mid i \leq n\} \to \{i \in \mathbb{N} \mid i \leq s\}$ כך ש-p_i ו-$q_{f(i)}$ הם חברים לכל $n \geq i \in \mathbb{N}$.

- ♣ במילים אחרות תחום שלמות ייקרא תחום פריקות חד-ערכית אם הוא מקיים את המשפט היסודי של האריתמטיקה.

3.4 תחומים ראשיים

הגדרה 3.18. R ייקרא תחום ראשי אם כל אידיאל שלו הוא אידיאל ראשי.

להביא דוגמאות לתחומי פח"ע שאינם תחומים ראשיים.

להביא דוגמאות לתחומים ראשיים שאינם תחומים אוקלידיים.

3.5 חוגים אוקלידיים

הגדרה 3.19. R ייקרא חוג אוקלידי (או תחום אוקלידי) אם קיימת פונקציה $N : R \setminus \{0\} \to \mathbb{N}_0$ המקיימת שלכל $a, b \in R$ כך ש-$b \neq 0$, קיימים $q, r \in R$ המקיימים $a = q \cdot b + r$, ובנוסף $N(r) < N(b)$ או ש-$r = 0$; N כזו תיקרא נורמה או דרגה.

- ♣ כמובן שההשראה להגדרה זו הגיעה מהחלוקה עם השארית הקיימת בחוג השלמים, שם פונקציית הערך המוחלט משמשת בתפקיד של N.
- ♣ הסיבה לשם "אוקלידי" היא שאלגוריתם אוקלידס תלוי ביכולת לחלק עם שארית, ומאלגוריתם זה נובעות רבות מן התכונות של השלמים.
- ♣ מבין כל החוגים שראינו עד כה החוגים האוקלידיים הם: כל שדה, חוג השלמים וכל חוג פולינומים מעל שדה.

3.6 חוג פולינומים מעל שדה

- ♣ ראו גם את הקובץ "על פולינומים".

[11] אנחנו עדיין תחת ההנחה ש-R הוא תחום שלמות, וכן בשתי ההגדרות הבאות (תחומים ראשיים וחוגים אוקלידיים).

4 שדות

♣ ראו גם את הקובץ "על שדות".

יהי $\mathbb{F}$ שדה.

הגדרה 4.1. המציין של $\mathbb{F}$ (נקרא גם המאפיין של $\mathbb{F}$) הוא הסדר של 1 בחבורה החיבורית של $\mathbb{F}$ כאשר סדר זה סופי, ואם אינו סופי יהיה המציין 0; בכל מקרה נסמן את המציין ב-$\operatorname{char}(\mathbb{F})$.

למה להגדיר את המציין להיות 0 ולא ∞? כך לא יהיה צורך לחלק למקרין וזה טבעי הרבה יותר.

טענה. $\operatorname{char}(\mathbb{F})$ הוא מספר ראשוני או ש-$\operatorname{char}(\mathbb{F})=0$.

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

הגדרה 4.2. השדה הראשוני של $\mathbb{F}$ הוא $\mathbb{F}_p$ אם $p:=\operatorname{char}(\mathbb{F})$ ראשוני, ואחרת יהיה $\mathbb{Q}$ השדה הראשוני של $\mathbb{F}$.