

שדות סופיים

[נכתב ע"י אוריה פירסט]

לפני שמתחילים

אם אתם:

לא יודעים מה זה מאפיין של שדה או

לא יודעים שהמאפיין הוא תמיד ראשוני או 0 או

לא יודעים שבשדה F ממאפיין $p > 0$ מתקיים $x^p = y^p = (x + y)^p$ או

לא יודעים שהמאפיין של שדה סופי הוא תמיד גדול מ-0,

אולי כדאי שתחזרו על החומר של קורסים קודמים או לפחות ודאו שאתם מבינים למה עובדות אלו

נכונות לפני שתקראו את המסמך.

אתם גם כנראה רוצים לדעת מה זה שדה פיצול.

מסמך זה פותח בתקציר עם עובדות עיקריות על שדות סופיים ללא הוכחה. לאחר מכן מובאות

ההוכחות של העובדות, לאו דווקא בסדר בו הוצגו.

תקציר

טענה ("קיום שדות סופיים"): יהי $q \in \mathbb{N}$.

1. קיים שדה בגודל q אם ורק אם $q = p^n$ עבור ראשוני p ו- n טבעי. במקרה זה המצוין של

השדה הוא \mathbb{Z}_p והשדה מכיל עותק של השדה $\mathbb{Z}/p\mathbb{Z} := \mathbb{Z}_p$ בתוכו.

2. במידה ו- $q = p^n$ כנ"ל, קיים רק שדה אחד בגודל q עד כדי איזומורפיזם (כלומר, אם F, F'

שני שדות בגודל q אז $F \cong F'$). מעתה נסמן שדה זה ב- \mathbb{F}_q .

הערה: שימו לב ש- $\mathbb{F}_p = \mathbb{Z}_p$ עבור ראשוני p , אבל $\mathbb{F}_{p^n} \neq \mathbb{Z}_{p^n}$ (כחוגים) עבור $n > 1$ כי \mathbb{Z}_{p^n} אינו

שדה.

טענה ("תתי שדות של שדות סופיים"): \mathbb{F}_q משוכן ב- $\mathbb{F}_{q'}$ אם ורק אם $q' = q^n$ עבור n שהוא.

בפרט, עבור ראשוני p , \mathbb{F}_p^n הוא תת שדה של \mathbb{F}_{p^m} אם ורק אם $n|m$.

טענה ("תורת גלואה של שדות סופיים"): אם $F \subseteq E$ שדות סופיים, אז E/F הרחבת גלואה

והחבורה $Gal(E/F)$ היא ציקלית ונוצרת ע"י ה- F איזומורפיזם $x \mapsto x^q$ כאשר $q = |F|$ (העתקה זו

גם נקראת אוטומורפיזם פרובניוס).

טענה ("מבנה החבורה הכפלית"): לכל שדה F ותת חבורה סופית G של (F^\times, \cdot) מתקיים כי G

היא ציקלית. בפרט, אם F שדה סופי אז החבורה (F^\times, \cdot) היא ציקלית.

טענה ("פולינומים אי פריקים מעל שדה סופי"): מעל השדה \mathbb{F}_q , הפולינום $x^{q^n} - x$ שווה למכפלת

כל הפולינומים המתוקנים האי פריקים מעל \mathbb{F}_q שמעלתם מחלקת את n . [בפרט, כל פולינום אי פריק

ממעלה n מעל \mathbb{F}_q מתחלק ב- $x^{q^n} - x$].

טענות עזר

לפני שנמשיך נצטרך טענות עזר.

טענת עזר 1: כל תחום שלמות סופי הוא שדה.

הוכחה: נשאיר את זה כתרגיל (שהייתם אמורים לראות באלגברה מופשטת 2).

טענת עזר 2: יהי F שדה ממאפיין $p > 0$ ויהי $n \in \mathbb{N}$. נגדיר $E = \{x \in F \mid x^{p^n} = x\}$. אזי E תת שדה סופי של F ו- $|E| \leq p^n$.

הוכחה: קודם נבדוק ש- E חוג. אם $x, y \in E$ אז $x^{p^n} = x, y^{p^n} = y$ ולכן $(x+y)^{p^n} = x^{p^n} + y^{p^n} = x + y$ ו- $(xy)^{p^n} = x^{p^n} y^{p^n} = xy$. כלומר, $xy, x+y \in E$. היות והמאפיין של F הוא $p > 0$ מתקיים $-x = (p-1) \cdot x \in E$. כלומר $-x \in E$. קיבלנו ש- E תת חוג של F ולכן גם תחום שלמות. אבל E הוא גם אוסף השורשים (ב- F) של הפולינום $x^{p^n} - x$ ולכן בהכרח $\deg(x^{p^n} - x) = p^n$. $|E| \leq \deg(x^{p^n} - x)$. כעת, לפי טענת עזר 1, E שדה וסיימנו. **משל.**

טענת עזר 3: יהי F שדה עם q איברים, אזי לכל $a \in F$ מתקיים $a^q = a$. בנוסף, $x^q - x = \prod_{a \in F} (x - a)$.

הוכחה: אם $a = 0$ זה ברור. אחרת, $a \in F^\times$. (F^\times, \cdot) היא חבורה בגודל $q-1$ ולכן לפי מסקנה ממשפט לגרנז' (ראו אלגברה מופשטת 1), $a^{q-1} = 1$. נכפול ב- a את שני האגפים וקיבלנו $a^q = a$. זה אומר שכל אברי F הם שורשים של $x^q - x$ ולכן $\prod_{a \in F} (x - a)$ מחלק אותו. היות והדרגות של שני הפולינומים שוות ושניהם מתוקנים, בהכרח $x^q - x = \prod_{a \in F} (x - a)$. **משל.**

טענת עזר 4: אם E/F הרחבת שדות סופיים אז $|E| = |F|^n$ כאשר $n = [E:F]$.

הוכחה: E הוא מרחב וקטורי מעל F ו- $n = [E:F] < \infty$. יהי $\{x_1, x_2, \dots, x_n\}$ בסיס ל- E מעל F . אזי כל איבר ב- E ניתן לכתוב בדיוק בדרך אחת כצירוף לינארי (מעל F) של $\{x_1, x_2, \dots, x_n\}$. לכן, מספר האיברים ב- E שווה למספר הצירופים הלינאריים השונים (מעל F) של $\{x_1, x_2, \dots, x_n\}$. אבל יש $|F|^n$ צירופים שונים כאלה ולכן $|E| = |F|^n$. **משל.**

הוכחות

טענה ("מבנה החבורה הכפלית"): לכל שדה F ותת חבורה סופית G של (F^\times, \cdot) מתקיים כי G היא ציקלית. בפרט, אם F שדה סופי אז החבורה (F^\times, \cdot) היא ציקלית.

הוכחה: נניח כי $|G| > 1$ (אחרת זה ברור). לפי משפט פירוק חבורות אבליות נוצרות סופית קיימים מספרים טבעיים d_1, d_2, \dots, d_r כך ש- $1 < d_1 \mid d_2 \mid \dots \mid d_r$ (כחבורות). קל לבדוק כי לכל איבר ב- $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_r}$ מתקיים $d_r \cdot x = 0$ ולכן נובע כי לכל $x \in G$ מתקיים $x^{d_r} = 1$. היות ו- $G \subseteq F$ זה אומר שלפולינום $x^{d_r} - 1$ יש $|G|$ שורשים שונים. אבל מעל שדה לפולינום ממעלה d_r יש לכל היותר d_r שורשים שונים ולכן $|G| \leq d_r$. לכן, בהכרח $|G| = d_r$ ואז $r = 1$ ו- $G \cong \mathbb{Z}_{d_1}$ היא ציקלית (כי \mathbb{Z}_{d_1} היא ציקלית). **משל.**

טענה ("קיום שדות סופיים"): יהי $q \in \mathbb{N}$.

- קיים שדה בגודל q אם ורק אם $q = p^n$ עבור ראשוני p ו- n טבעי. במקרה זה המצוין של השדה הוא p והשדה מכיל עותק של השדה $\mathbb{Z}/p\mathbb{Z} := \mathbb{Z}_p$ בתוכו.
- במידה ו- $q = p^n$ כנ"ל, קיים רק שדה אחד בגודל q עד כדי איזומורפיזם (כלומר, אם F, F' שני שדות בגודל q אז $F \cong F'$). מעתה נסמן שדה זה ב- \mathbb{F}_q .

הוכחת 1: כווננו כי F שדה בגודל q . יהי $F_0 = \{n \cdot 1 \mid n \in \mathbb{Z}\}$ (בסימון $n \cdot 1$ הכוונה היא ל- $1 + 1 + \dots + 1$ כאשר 1 מופיע n פעמים). F_0 הוא חוג סופי (בדקו) ולפי הגדרת המאפיין של שדה,

$char F = |F_0|$. נגדיר $p = |F_0|$ (שימו לב ש- p ראשוני). היות ו- F_0 תת חוג של F , F_0 הוא תחום שלמות. כעת לפי טענת עזר 1, F_0 שדה והוא איזומורפי ל- \mathbb{Z}_p (תרגיל). קיבלנו ש- F מכיל עותק של \mathbb{Z}_p (מעכשיו נמשיך כאילו $\mathbb{Z}_p \subseteq F$). לכן, לפי טענת עזר 4, $q = |F| = p^n$ (באשר $n = [F:\mathbb{Z}_p]$), כדורש.

כונן ב: נניח כי $q = p^n$ עבור p ראשוני. יהי E שדה הפיצול של $x^{p^n} - x$ מעל \mathbb{Z}_p ויהי $F = \{x \in E \mid x^{p^n} - x = 0\}$. לפי טענת עזר 2, F שדה ו- $|F| \leq p^n$. כעת, נשים לב שמתקיים $\gcd(x^{p^n} - x, (x^{p^n} - x)') = 1$ ולכן $x^{p^n} - x$ ספרבילי. זה אומר של- $x^{p^n} - x$ יש p^n שורשים שונים ב- E ולכן $|F| \geq p^n$. לכן, בהכרח $|F| = p^n$ ו- F שדה עם $q = p^n$ איברים. **משל.**

הוכחת 2: יהיו F, F' שני שדות בגודל $q = p^n$. לפי סעיף ניתן להניח כי \mathbb{Z}_p מוכל ב- F וב- F' . נתבונן ב- F . לפי טענת עזר 3, $x^q - x$ מתפצל לגורמים לינאריים מעל F . הוא לא יכול להתפצל לגורמים לינאריים מעל אף תת שדה של F (כי חייבים להיות לפחות q איברים בשדה מעליו $x^q - x$ מתפצל) ולכן F שדה פיצול של $x^q - x$ מעל \mathbb{Z}_p . באותו אופן, גם F' הוא שדה פיצול של $x^q - x$ מעל \mathbb{Z}_p . כעת, מיחידות שדה הפיצול נובע $F \cong F'$. **משל.**

טענה ("תורת גלואה של שדות סופיים"): אם $F \subseteq E$ שדות סופיים, אז E/F הרחבת גלואה והחבורה $Gal(E/F)$ היא ציקלית ונוצרת ע"י ה- F איזומורפיזם $x \mapsto x^q$ (העתקה זו גם נקראת אוטומורפיזם פרובניוס).

הוכחה: יהי p המאפיין של F , אזי q הוא חזקה של p ולכן ההעתקה $\phi(x) = x^q$ היא הומומורפיזם שדות. ϕ היא אוטומורפיזם כי היא חח"ע מקבוצה סופית לעצמה¹. לפי טענת עזר 3, $\phi(x) = x$ לכל $x \in F$ ולכן $\phi \in Gal(E/F)$. תהי G תת החבורה הנוצרת ע"י ϕ ב- $Gal(E/F)$, אזי $E^G \subseteq E^{\langle \phi \rangle} = F$ ולכן $\{x \in E \mid x^q = x\} = F$ (השוויון האחרון נובע מטענת עזר 3). לכן $F = E^G$ ולפי התאמת גלואה נקבל ש- $Gal(E/E^G) = Gal(E/F) = G = \langle \phi \rangle$. **משל.**

טענה ("תתי שדות של שדות סופיים"): \mathbb{F}_q משוכן ב- $\mathbb{F}_{q'}$ אם ורק אם $q' = q^n$ עבור n שהוא בפרט, עבור ראשוני p , \mathbb{F}_{p^n} הוא תת שדה של \mathbb{F}_{p^m} אם ורק אם $n|m$.

הוכחה: כונן א: נניח ש- $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$, אזי $\mathbb{F}_{q'}$ מרחב וקטורי מעל \mathbb{F}_q . כעת, לפי טענת עזר 4, $q' = q^n$ עבור n כלשהו.

כונן ב: נניח ש- $q' = q^n$ ונראה של- $\mathbb{F}_{q'}$ יש תת שדה בגודל q . מתקיים:

$$\begin{aligned} x^{q'} - x &= x(x^{q^{n-1}} - 1) = x(x^{q-1} - 1)(x^{q^{n-2}} + x^{q^{n-3}} + \dots + x^q + 1) = \\ &= (x^q - x)(x^{q^{n-2}} + x^{q^{n-3}} + \dots + x^q + 1) \end{aligned}$$

ולכן $x^q - x \mid x^{q'} - x$. לפי טענת עזר 3, $x^{q'} - x$ מתפצל לגורמים לינאריים שונים מעל $\mathbb{F}_{q'}$ ולכן גם $x^q - x$ מתפצל לגורמים לינאריים שונים. זה אומר שבקבוצה $E = \{x \in \mathbb{F}_{q'} \mid x^q = x\}$ יש בדיוק q איברים שונים. כעת, לפי טענת עזר 2, E תת שדה של $\mathbb{F}_{q'}$ בגודל q . **משל.**

טענה ("פולינומים אי פריקים מעל שדה סופי"): מעל השדה \mathbb{F}_q , הפולינום $x^{q^n} - x$ שווה למכפלת כל הפולינומים המתוקנים האי פריקים מעל \mathbb{F}_q שמעלתם מחלקת את n . [בפרט, כל פולינום אי פריק ממעלה n מעל \mathbb{F}_q מתחלק ב- $x^{q^n} - x$].

¹ יש שדות אינסופיים ממאפיין p עבורים ϕ אינה חד חד ערכית.

הוכחה: יהי $f \in \mathbb{F}_q[x]$ פולינום אי פריק ממעלה d המחלקת את n . אזי $E = \mathbb{F}_q[x]/\langle f \rangle$ הוא שדה ממימד d מעל \mathbb{F}_q ולפי טענת עזר 4 מכיל p^d איברים. לכן, יש עותק של E ב- \mathbb{F}_{q^n} . זה אומר של- f יש שורש ב- \mathbb{F}_{q^n} . כל אברי \mathbb{F}_{q^n} הם שורשים של $x^{q^n} - x$ (טענת עזר 3) ולכן נובע ש- $f \mid x^{q^n} - x$. לפיכך, $x^{q^n} - x$ מתחלק במכפלת כל הפולינומים המתוקנים האי פריקים מעל \mathbb{F}_q שמעלתם מחלקת את n . כדי לסיים נראה כי מתקיים ההיפך – מכפלת כל הפולינומים הנ"ל מתחלקת ב- $x^{q^n} - x$.

לכל $a \in \mathbb{F}_{q^n}$ נסמן ב- f_a את הפולינום המינימלי של a מעל \mathbb{F}_q ונגדיר $S = \{f_a \mid a \in \mathbb{F}_{q^n}\}$. כל איבר ב- \mathbb{F}_{q^n} הוא שורש של אחד הפולינומים ב- S . לכן, $x^{q^n} - x = \prod_{a \in \mathbb{F}_{q^n}} (x - a)$ (טענת עזר 3) מחלק את $\prod_{f \in S} f$. לכל $a \in \mathbb{F}_{q^n}$ מתקיים ש- f_a אי פריק ו- $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] \mid [\mathbb{F}_q[a] : \mathbb{F}_q] = \deg f_a$. לכן, $\prod_{f \in S} f$ מחלק את מכפלת כל הפולינומים המתוקנים האי פריקים מעל \mathbb{F}_q שמעלתם מחלקת את n וגמרנו. **משל.**