שדות סופיים

אם F שדה סופי, $char(F)=p$ ראשוני. לכן $\mathbb{F}_p \subseteq F$, לכן F מרחב וקטורי מעל $\mathbb{F}_p$. אם $[F:\mathbb{F}_p]=n$, אז $|F|=p^n$.

לכל $q=p^n$ קיים שדה סופי מסדר q, שמסומן $\mathbb{F}_q$ (ולפעמים $GF(q)$). הוא יחיד עד כדי איזומורפיזם.

תרגיל:

הוכיחו שבשדה $\mathbb{F}_q$ מתקיים

$$x^q - x = \prod_{a\in\mathbb{F}_q}(x-a).$$

הוכחה:

אם $a=0$, a הוא שורש של x^q-x.

אם $a\neq 0$, אז $a\in\mathbb{F}_q^\times$ שהיא חבורה מסדר $q-1$, ולפי משפט אוילר מתורת החבורות נקבל $a^{q-1}=1 \Leftarrow a^q=a$.

זה מראה שכל $a\in\mathbb{F}_q$ הוא שורש של x^q-x. לכן $\prod_{a\in\mathbb{F}_q}(x-a) \mid x^q-x$, וכיוון שהם מאותה מעלה ומתוקנים, הפולינומים שווים.

$\square$

הערות:

א. $\mathbb{F}_q^\times$ ציקלית מסדר $q-1$.

ב. החבורה החיבורית $\mathbb{F}_q$ (אם $q=p^n$) איזומורפית ל-$(\mathbb{Z}/p\mathbb{Z})^n$.

ג. כל הרחבה של שדות סופיים היא גלואה וציקלית.

לדוגמה, אם $q=p^n$, אז $Gal(\mathbb{F}_q/\mathbb{F}_p)\cong\mathbb{Z}/n\mathbb{Z}$, ויוצר של זה לדוגמה הוא

אוטומורפיזם פרובניוס: $\sigma: x \longmapsto x^p$.

3. מהתרגיל הקודם, $\mathbb{F}_q$ שדה הפיצול של x^q-x מעל $\mathbb{F}_p$.

תרגיל:

בנו במפורש שדה בן 8 איברים.

פתרון:

השדה הזה הוא שדה הפיצול של x^8-x.

$$\left[\mathbb{F}_2[x]\big/\langle f(x)\rangle \quad \deg f(x)=3 \text{ אי-פריק}\right]$$

$$x^8-x = x(x^7-1) = x(x-1)(x^6+x^5+\dots+x+1) =$$
$$= x(x-1)(x^3+x+1)(x^3+x^2+1)$$

נשים לב ש- x^3+x+1 וגם x^3+x^2+1 אי-פריקים מעל $\mathbb{F}_2$, כי הם ממעלה 3 ואין להם שורשים. לכן השדה שלנו איזומורפי ל- $\mathbb{F}_2[x]\big/\langle x^3+x+1\rangle$.

$\square$

תרגיל:

יהי F אחד מהשדות $\mathbb{F}_3$, $\mathbb{F}_5$ ו- $\mathbb{F}_7$. מצאו את מימד שדה הפיצול של x^3-2 מעל F, ותארו את הפעולה של האוטומורפיזם היוצר את חבורת גלואה.

פתרון:

$\boxed{\mathbb{F}_3}$ הפולינום מתפרק בצורה $x^3-2=(x-2)^3$.

לכן שדה הפיצול שלו הוא $\mathbb{F}_3$, ממימד 1, וחבורת גלואה טריוויאלית.

$$\boxed{\begin{array}{c}\text{במאפיין } p\text{,}\\ (a+b)^p=a^p+b^p\\ \text{(העתקת פרובניוס)}\end{array}}$$

$\boxed{\mathbb{F}_5}$ הפולינום מתפרק $x^3-2=(x-3)(x^2+3x+4)$

והפולינום x^2+3x+4 אי-פריק (ממעלה 2 בלי שורשים).

$\Leftarrow$ שדה הפיצול של x^3-2 = E = שדה הפיצול של x^2+3x+4.

לכן גם הרחבה ממימד 2, כלומר $E\cong\mathbb{F}_{25}$. חבורת גלואה

$$Gal(\mathbb{F}_{25}/\mathbb{F}_5)\cong\mathbb{Z}/2\mathbb{Z}$$

$$\boxed{\mathbb{F}_5[x]/\langle x^2+3x+4\rangle}$$

איברי השדה הם מהצורה $a+bx\in\mathbb{F}_5[x]$ כאשר $x^2=-3x-4$.

אוטומורפיזם פרובניוס $\varphi: x\mapsto x^5$ פועל לפי

$$\varphi(a+bx)=a+bx^5=a+bx\cdot x^2\cdot x^2=a+bx(-3x-4)(-3x-4)=$$
$$=a+bx(4x^2+4x+1)=a+bx(-12x-16+4x+1)=$$
$$=a+bx\cdot 2x=a+2bx^2=a+2b(-3x-4)=a+2b+4bx$$

$\boxed{\mathbb{F}_7}$ הפולינום x^3-2 אי-פריק. אפשר לוודא עם שורשים על ידי הצבה.

דרך אחרת: אם α שורש של x^3-2, אז $\alpha^3=2 \Downarrow \alpha^6=4$

אבל ממשפט אוילר צריך $\alpha^6=1$, בסתירה.

לכן $\mathbb{F}_{7^3}\cong\mathbb{F}_7[x]/\langle x^3-2\rangle$ שדה הפיצול של x^3-2 מעל $\mathbb{F}_7$.

$\Leftarrow$ המימד הוא 3, $Gal(\mathbb{F}_{7^3}/\mathbb{F}_7)\cong\mathbb{Z}/3\mathbb{Z}$.

במפורש, איברי השדה הם $a+bx+cx^2\in\mathbb{F}_7[x]$ כך ש- $x^3=2$.

פעולת אוטומורפיזם פרובניוס: $\varphi: x\mapsto x^7$

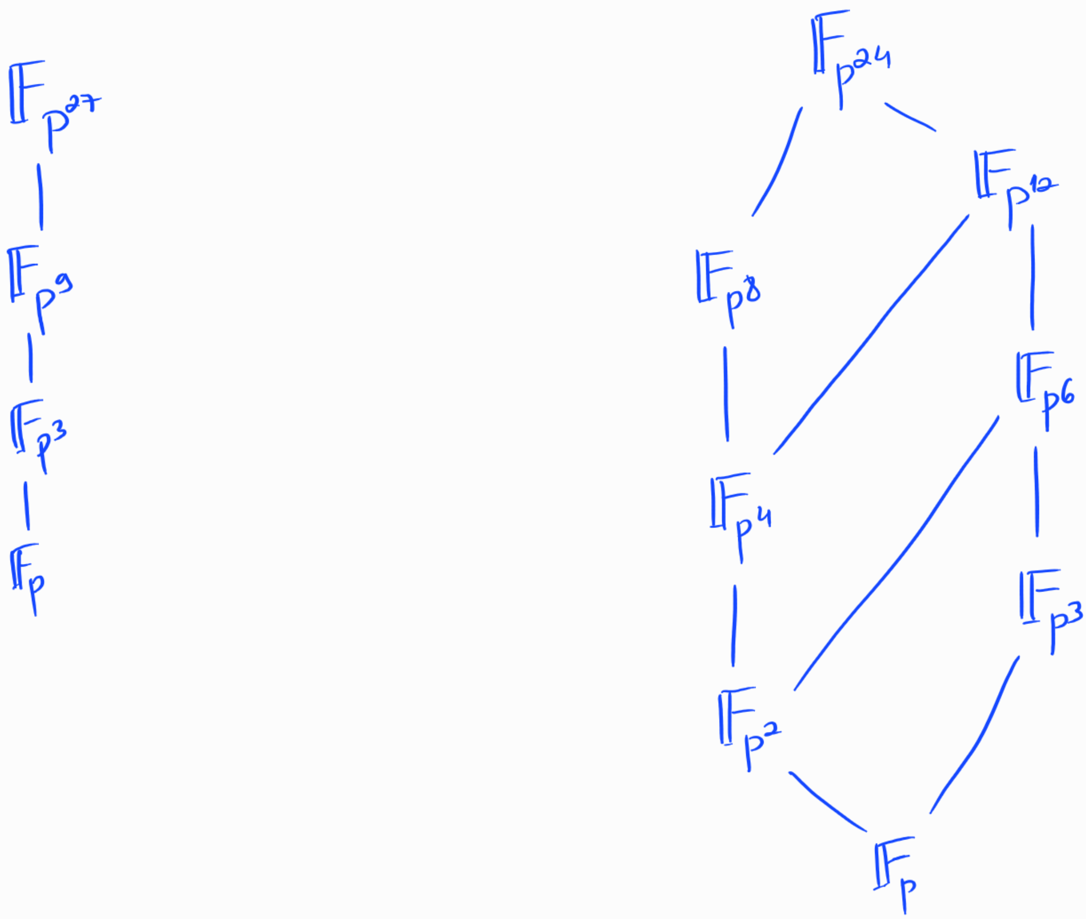
$$\varphi(a+bx+cx^2)=a+bx^7+cx^{14}\underset{\uparrow}{=}a+4bx+2cx^2$$

$$x^7=x\cdot x^6=x\cdot(x^3)^2=4x$$
$$x^{14}=(x^7)^2=16x^2=2x^2$$

משפט:

$\mathbb{F}_q$ הוא תת-שדה של $\mathbb{F}_t$ $\iff$ $t=q^k$ לאיזשהו k.

בפרט, אם p ראשוני, $\mathbb{F}_{p^m}$ תת-שדה של $\mathbb{F}_{p^n}$ $\iff$ $n|m$.



משפט:

ב-$\mathbb{F}_p$,

$$x^{p^n}-x=\prod_{\substack{f\in\mathbb{F}_p[x] \text{ אי-פריק} \\ \text{ממעלה שמחלקת} \\ \text{את } n}} f(x)$$

בפרט אם $f\in\mathbb{F}_p[x]$ אי-פריק ממעלה n, הוא מתפצל ב-$\mathbb{F}_{p^n}$.

תרגיל: (ממבחן)

מצאו כמה פולינומים אי-פריקים יש ממעלה 4 מעל $\mathbb{F}_2$.

פתרון:

נחשב ראשית למעלות 1 ו-2.

הפולינומים האי-פריקים ממעלה 1 הם $x, x+1$. לכן יש שניים.

כמה פולינומים אי-פריקים ממעלה 2 יש?

$$x^{2^2}-x = x(x+1)\cdot(x^2+x+1)$$

לכן יש פולינום אי-פריק יחיד ממעלה 2 מעל $\mathbb{F}_2$.

$$x^{16}-x = x^{2^4}-x = x(x+1)(x^2+x+1)\cdot g_4(x)$$

כאשר $g_4(x)$ מכפלת כל האי-פריקים מעל $\mathbb{F}_2$ ממעלה 4.

$\deg g_4(x)=12 \Leftarrow$ ישנם בדיוק $\underset{12/4}{\overset{\shortparallel}{3}}$ פולינומים אי-פריקים ממעלה 4 מעל $\mathbb{F}_2$.

תרגיל:

בהמשך לתרגיל הקודם, כמה פולינומים אי-פריקים ממעלה 8 יש מעל $\mathbb{F}_2$?

פתרון:

$$x^{2^8}-x = \prod_{\substack{f\in\mathbb{F}_2[x] \text{ אי-פריק} \\ \text{ממעלה שמחלקת את } 8}} f(x) = (x^{2^4}-x)\cdot \underbrace{\prod_{\substack{f\in\mathbb{F}_2[x] \text{ אי-פריק} \\ \text{ממעלה } 8}} f(x)}_{g_8(x)}$$

לכן $g_8(x) = \dfrac{x^{2^8}-x}{x^{2^4}-x}$. $\deg g_8(x) = 2^8-2^4=240$. לכן יש $\frac{240}{8}=30$ פולינומים אי-פריקים ממעלה 8 מעל $\mathbb{F}_2$.