דוגמא: נקח $x^4-2\in\mathbb{Q}[x]$, ו-$\mathbb{C}$ הרחבה של $\mathbb{Q}$.

$$x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-i\sqrt[4]{2})(x+i\sqrt[4]{2})$$

לכן $K\equiv\mathbb{Q}(\sqrt[4]{2},-\sqrt[4]{2},i\sqrt[4]{2},-i\sqrt[4]{2})$ הוא שדה פיצול מינימלי של x^4-2.

נשים לב שמתקיים: $K=L\equiv\mathbb{Q}(i,\sqrt[4]{2})$.

(4 השורשים של x^4-2 נמצאים ב-L, ולכן מלמה קודמת $K\subseteq L$.

מצד שני $i,\sqrt[4]{2}$ נמצאים ב-K, ולכן מלמה קודמת $L\subseteq K$.)

מסקנה: יהי $F\subset L$ ויהיו $\alpha_1,\dots,\alpha_n\in L$. אז לכל $1\le r\le n-1$ מתקיים:

$$(\mathbb{F}(\alpha_1,\dots,\alpha_r))(\alpha_{r+1},\dots,\alpha_n)=\mathbb{F}(\alpha_1,\dots,\alpha_n)$$

למה: נניח כי $F\subset L$ הרחבה של שדות. יהי $\alpha\in L$ אלגברי מעל F, ויהי $p\in\mathbb{F}[x]$ הפולינום המינימלי של α. אז קיים איזומורפיזם **יחיד** של חוגים $\psi:\mathbb{F}[\alpha]\to\mathbb{F}[x]/\langle p\rangle$ שקבוע על F והשולח את α לקוסט $x+\langle p\rangle$.

$\forall x\in\mathbb{F}:\ \psi(x)=x$

מסקנה: p אי פריק $\Leftarrow$ $\mathbb{F}[x]/\langle p\rangle$ שדה $\Leftarrow$ $\mathbb{F}[\alpha]$ שדה! (בהנחה ש-α אלגברי מעל $\mathbb{F}$)

הוכחת הלמה: נגדיר העתקה $\varphi:\mathbb{F}[x]\to L$ ע"י $\varphi(h(x))=h(\alpha)$. קל לראות כי φ הומומורפיזם של חוגים. מהגדרה, התמונה של φ היא $\operatorname{Im}\varphi=\mathbb{F}[\alpha]$. נראה כי $\ker\varphi=\langle p\rangle$. ~~יהי $g\in\mathbb{F}[x]$~~

יהי $g\in\mathbb{F}[x]$.
$$\varphi(gp)=\varphi(g)\varphi(p)=g(\alpha)p(\alpha)=0$$

לכן $\langle p\rangle\subseteq\ker\varphi$. יהי $f\in\ker\varphi$. אז $\varphi(f)=f(\alpha)=0$ - מלמה שהוכחנו, $p\mid f$ (p מינימלי של α) ולכן $\cancel{f}=pg$ ולכן $f\in\langle p\rangle$. כלומר $\ker\varphi\subseteq\langle p\rangle$. $\Leftarrow$ $\ker\varphi=\langle p\rangle$.

ממשפט האיזומורפיזם I: $\mathbb{F}[x]/\ker\varphi\cong\operatorname{Im}\varphi$ $\Leftarrow$ $\mathbb{F}[x]/\langle p\rangle\cong\mathbb{F}[\alpha]$.

φ קבועה על $\mathbb{F}$ ושולחת את $x+\langle p\rangle$ ל-α.

יחידות נובעת כי כל הומומורפיזם מ-$\mathbb{F}[\alpha]$ נקבע באופן יחיד ע"י הערכים של α ואיברי $\mathbb{F}$. $\square$

תרגול 3

תרגיל: נניח כי $f(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}[x]$ ונניח כי $\frac{r}{s}$ הוא שורש של $f(x)$, וגם $\gcd(r,s)=1$.

אז $r\mid a_0$ ו-$s\mid a_n$.

תרגיל: הוכח כי x^4-10x^2+1 אי פריק מעל $\mathbb{Q}$.

פתרון: כיוון שהפולינום מתוקן, אין לו שורש רציונלי פרט להם שלמים.

קל לראות כי $1,2,3$ לא שורשים ו-$x^4-10x^2+1>0$ עבור $x\ge 4$.

אז אין לו שורשים ב-$\mathbb{Q}$. נניח כי: $(x^2+ax+b)(x^2+cx+d)=x^4-10x^2+1$.

השוואת מקדם x^3 נותן: $a=-c$. $(x^4-10x^2+1)=(x^2+ax+b)(x^2-ax+c)$

מקדם חופשי: $bc=1$. מקדם של x^2: $c+b-a^2=-10$. של x: $ac=ab$.

אז $a\neq c$ ⇐ $b=c$. , $bc=1$ ⇐ $b=c=1$ או $b=c=-1$. $b+c-a^2=10$ ⇐ $a^2=12$

או $a^2=8$. אין פתרונות שלמים. □

<u>תרגיל</u>: x^5-x^2+1 אי פריק מעל $\mathbb{Q}$.

<u>פתרון</u>: נזכור כי אם $f(x)$ פריק מעל $\mathbb{Z}$ אז הוא פריק מעל $\mathbb{Z}_p$, p ראשוני. (אם נשמרת הדרגה)

נקח $p=2$. שם הוא פריק אם חייב להופיע גורם לינארי או ריבועי.

האי־פריקים הלינאריים ב־$\mathbb{Z}_2$ הם x או $x+1$. הריבועיים: x^2, x^2+x, x^2+x+1,

x^2+1. קל לבדוק כי 6 הפולינומים האלו לא מחלקים את x^5-x^2+1. לכן x^5-x^2+1

אי־פריק מעל $\mathbb{Z}_p$ ⇐ x^5-x^2+1 אי פריק מעל $\mathbb{Z}$. □

<u>טענה</u>: נניח כי $f(x)=a_0+a_1x+\dots+a_nx^n$ אי־פריק מעל שדה $\mathbb{F}$. ~~אזי~~ אזי $\tilde{f}(x)=a_n+a_{n-1}x+\dots+a_0x^n$

אי־פריק מעל $\mathbb{F}$.

<u>הוכחה</u>: נניח: $\tilde{f}(x)=\tilde{a}(x)\tilde{b}(x)$, כאשר $\deg\tilde{b}=l$, $\deg\tilde{a}=m$, $m+l=n$.

בחוג המנות $\mathbb{F}(x)$ נקבל: $x^{-n}\tilde{f}(x)=x^{-m}\tilde{a}(x)x^{-l}\tilde{b}(x)$. (1)

כמו כן ב־$\mathbb{F}(x)$ מתקיים: $x^{-n}\tilde{f}(x)=f(\frac{1}{x})$ ומ־(1):

$f(\frac{1}{x})=a(\frac{1}{x})b(\frac{1}{x})$.

ההעתקה (*) $p(x)\mapsto p(\frac{1}{x})$ הינה ~~[illegible]~~ אוטומורפיזם מ־$\mathbb{F}(x)$ לעצמו. לכן:

$f(x)=a(x)b(x)$. אז $l=0$ או $m=0$. ⇐ $\tilde{f}(x)$ אי־פריק. □

<u>תרגיל</u>: יהי $n\geq 2$, p ראשוני: $f(x)=x^n+px+p^2$ אי־פריק מעל $\mathbb{Q}$.

<u>פתרון</u>: נניח: $f(x)=a(x)b(x)$, ונקח מודולו p. $\tilde{a}(x)\tilde{b}(x)=\tilde{f}(x)=x^n$ ⇐

$\tilde{a}(x)=x^s$, $\tilde{b}(x)=x^t$. לכן: $a(x)=x^s+\sum_{k=0}^{s-1}pa_kx^k$, $b(x)=x^t+\sum_{k=0}^{t-1}pb_kx^k$

<u>מקרה 1</u>: $s=1$ (או $t=1$).

$$f(x)=(x+pa_0)(x^t+\dots+pb_0)=x^n+px+p^2$$

ע״י השוואת מקדמים חופשיים: $a_0b_0=1$ ⇐ $a_0=\pm1$ ⇐ $x=\pm p$ הוא שורש של

$f(x)$, סתירה.

<u>מקרה 2</u>: $s\geq 2$, $t\geq 2$. אז המקדם של x הוא:

$p^2a_1b_0+p^2a_0b_1$, כפולה של p^2. סתירה. □