דוגמה: נבנה שדה בן 4 איברים. נפרק את x^4-x מעל $\mathbb{Z}_2$.

$$x^4-x = x(x-1)(x^2+x+1)$$

מתרגיל 2, שאלה 7, נקבל שכל אחד מ-3 הפולינומים האלו אי-פריק מעל $\mathbb{Z}_2$.
יהי α שורש של x^2+x+1 בשדה הרחבה כלשהו. אז איברי השדה $\mathbb{Z}_4$ יהיו
$0, 1, \alpha, \alpha+1$. הפעולות מתבצעות הן מודולו $\mathbb{Z}_2$ ותוך כדי שימוש בעובדה ש $\alpha^2+\alpha+1=0$
לדוג: $\alpha^2=-\alpha-1=\alpha+1$, $\alpha(\alpha+1)=\alpha^2+\alpha=-1=1$, $\alpha+\alpha=0$, $\alpha+(\alpha+1)=1$ וכו'.

אי-פריקות של פולינומים

נחפש קריטריונים מתי פולינום אי-פריק מעל תחום שלמות, למשל $\mathbb{Z}$.

טענה: אם $\sigma: R\to S$ הומומורפיזם של חוגים, אז ההעתקה $\sigma^*: R[x]\to S[x]$ המוגדרת ע"י:

$$\sigma^*\left(\sum a_i x^i\right) = \sum \sigma(a_i) x^i$$

היא גם הומומורפיזם של חוגים.

משפט: יהי R תחום שלמות ו-F שדה. יהי $\sigma: R\to F$ הומומורפיזם של חוגים, ויהי $p(x)\in R[x]$.
אם $\deg(\sigma^*(p))=\deg(p)$ וגם $\sigma^*(p)$ פולינום אי-פריק ב-$F[x]$, אז $p(x)$ הינו אי-פריק ב-$R[x]$.

הוכחה: נניח כי $p(x)=f(x)g(x)$ עם $\deg g, \deg f < \deg p$ (בשלילה).
אז ב-$F[x]$ מתקיים (σ^* הומומורפיזם). $\sigma^*(p)=\sigma^*(f)\cdot\sigma^*(g)$.
ומכיוון ש-$\sigma^*(p)$ אי-פריק, ניתן להניח כי $\deg\sigma^*(f)=0$.

$$\deg(p) \underset{\text{נתון}}{=} \deg(\sigma^*(p)) = \deg(\sigma^*(f)) + \deg(\sigma^*(g)) = \deg(\sigma^*(g)) \le$$
$$\le \deg(g) < \deg(p)$$

סתירה! ($\deg(p)<\deg(p)$). לכן ההנחה שגויה, כלומר $p(x)$ אי-פריק. □

דוגמאות: 1) $f(x)=8x^3-6x-1\in\mathbb{Z}[x]$. נבחן את $\sigma:\mathbb{Z}\to\mathbb{Z}_p$ כאשר p ראשוני המוגדרת
ע"י שארית מודולו p הינה הומומורפיזם בין חוגים.
אם $p=2$, $\deg f > \deg\sigma^*(f)$, אסור להשתמש במשפט.
אם $p=3$, $\sigma^*(f)=-(x^3+1)$, כאן $\sigma^*(f)$ פריק.
אם $p=5$ נקבל $\sigma^*(f)=3x^3-x-1$. קל לראות שפולינום זה אי-פריק. לכן מהמשפט,
$f(x)$ אי-פריק ב-$\mathbb{Z}[x]$.
2) קל לראות כי $f(x)=x^4-10x^2+1$ אי פריק מעל $\mathbb{Q}[x]$ ולכן מעל $\mathbb{Z}[x]$.
לעומת זאת מודולו כל ראשוני p, $f(x)$ פריק.

הגדרה: פולינום $f(x)$ ב-$\mathbb{Z}[x]$ ייקרא פרימיטיבי אם ה-gcd של כל מקדמיו הוא 1.
אם d הינו ה-gcd של כל מקדמי פולינום, $\frac{1}{d}f(x)$ הינו פרימיטיבי.

למה (הלמה של Gauss) המכפלה של שני פולינומים פרימיטיביים הוא פולינום פרימיטיבי.

הוכחה נניח כי $f(x), g(x)$ פרימיטיביים ו-$f(x)g(x)$ לא פרימיטיבי. לכן קיים ראשוני p המחלק את כל מקדמי הפולינום. נגדיר: $\sigma : \mathbb{Z} \to \mathbb{Z}_p$, ע"י שארית מודולו p. σ הומומורפיזם.

אז מתקיים: $0 = \sigma^*(fg) \equiv \sigma^*(f)\sigma^*(g)$.

זהו שוויון ב-$\mathbb{Z}_p[x]$. כיוון ש-$\mathbb{Z}_p[x]$ תחום שלמות, אין מחלקי 0, אז $\sigma^*(f)=0$, או $\sigma^*(g)=0$. אבל כיוון ש-f, g פרימיטיביים, $\sigma^*(f)\neq 0$ וגם $\sigma^*(g)\neq 0$. סתירה.
□

למה לכל פולינום $f(x)\in\mathbb{Q}[x]$ ישנו פירוק יחיד מהצורה: $f(x)=c(f)\cdot f^*(x)$, כאשר $c(f)\in\mathbb{Q}$ מספר חיובי ו-$f^*(x)\in\mathbb{Z}[x]$ הינו פרימיטיבי.

הגדרה המספר $c(f)$ נקרא התוכן (content) של $f(x)$.

הוכחה: נניח: $f(x)=\sum_{i=0}^{n}\frac{a_i}{b_i}x^i$ כאשר $a_i,b_i\in\mathbb{Z}$.

נסמן: $B=b_0b_1\cdots b_n$. אז $g(x)=Bf(x)\in\mathbb{Z}[x]$.

נסמן: $D=\pm d$ כאשר d הינו gcd של כל מקדמי $g(x)$, והסימן נקבע כך ש $\frac{B}{D}>0$.

מתקיים: $\frac{B}{D}f(x)=\frac{1}{D}g(x)\in\mathbb{Z}[x]$ וזהו גם פולינום פרימיטיבי. נגדיר $c(f)=\frac{D}{B}$

ואילו $f^*(x)=\frac{B}{D}f(x)$.

נותר להוכיח יחידות. נניח כי $f(x)=e\,h(x)$ הינו פירוק כנ"ל כך ש-$e>0$ וגם $h(x)\in\mathbb{Z}[x]$ פרימיטיבי. אזי $c(f)f^*(x)=f(x)=e\cdot h(x)$. ולכן:

$$f^*(x)=\frac{e}{c(f)}\cdot h(x).$$

נרשום את $\frac{e}{c(f)}$ כ-$\frac{u}{v}$ כך ש-$\gcd(u,v)=1$, $u,v\in\mathbb{N}$. אז ב-$\mathbb{Z}[x]$ נקבל את השוויון $v\,f^*(x)=u\,h(x)$. מהשוואת מקדמים נקבל כי v מחלק את כל מקדמי $uh(x)$, כיוון ש $(u,v)=1$, אז v מחלק את כל מקדמי $h(x)$ וכיוון ש-$h(x)$ פרימיטיבי $v=1$. באופן דומה $u=1$.
□

מסקנה אם $f(x)\in\mathbb{Z}[x]$, אז $c(f)\in\mathbb{Z}$.

הוכחה יהי d ה-gcd של כל מחלקי f, אז $\frac{1}{d}f(x)\in\mathbb{Z}[x]$ ופרימיטיבי. מיחידות הפירוק, $f^*(x)=\frac{1}{d}f(x)$, $c(f)=d\in\mathbb{Z}$.
□

מסקנה אם $f(x)\in\mathbb{Q}[x]$ וגם $f(x)=g(x)h(x)$ כאשר $g,h\in\mathbb{Q}[x]$ אז $c(f)=c(g)c(h)$,

ו- $f^*(x)=g^*(x)\cdot h^*(x)$

הוכחה $f(x)=g(x)h(x)=(c(g)\cdot g^*(x))\cdot(c(h)\cdot h^*(x))=c(g)\cdot c(h)\cdot \underbrace{g^*(x)\cdot h^*(x)}$

מהלמה של Gauss g^*h^* פרימיטיבי ו- $c(g)\cdot c(h)$ רציונלי חיובי. אז מיחידות הפירוק,

המסקנה נובעת. □

משפט (Gauss) אם לא ניתן לרשום את $p(x)$ כמכפלה של 2 פולינומים ב-$\mathbb{Z}[x]$ שדרגתם קטנה ממש מזו של $p(x)$, אזי $p(x)$ אי פריק ב-$\mathbb{Q}[x]$.

הוכחה נניח כי $p(x)=g(x)\cdot h(x)$ ב-$\mathbb{Q}[x]$. אזי מתקיים:

$$p(x)=c(g)c(h)g^*(x)h^*(x)$$

כאשר $g^*,h^*\in\mathbb{Z}[x]$. מתקיים מהלמה הקודמת: $c(g)=c(h)=c(p)$. $c(p)\in\mathbb{Z}$, כי $p\in\mathbb{Z}[x]$.
אזי $p(x)=(c(p)g^*(x))h^*(x)$ פירוק מעל $\mathbb{Z}[x]$. סתירה. □

מסקנה פולינום $p(x)\in$ אי פריק מעל $\mathbb{Z}(x)$ $\Rightarrow$ $p(x)$ אי פריק מעל $\mathbb{Q}[x]$.

משפט: (קריטריון Eisenstein) $f(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}[x]$. נניח קיים ראשוני p המחלק את כל ה-a_i-ים לכל $i<n$, $p\nmid a_n$, וגם $p^2\nmid a_0$, אזי $f(x)$ אי-פריק מעל $\mathbb{Z}[x]$. (ולכן מעל $\mathbb{Q}[x]$)

הוכחה נניח כי $f(x)=g(x)h(x)=(\sum_{i=0}^{m}b_ix^i)(\sum_{j=0}^{k}c_jx^j)$, $g,h\in\mathbb{Q}[x]$.
ממשפט גאוס, ניתן להניח כי $g,h\in\mathbb{Z}[x]$ (כל פירוק גורר פירוק מעל $\mathbb{Z}[x]$).
מהנתון: $p\mid a_0=b_0c_0$. לכן $p\mid b_0$ או $p\mid c_0$. כיוון ש-$p^2\nmid a_0$, אז נוכל להניח כי $p\mid c_0$ אבל $p\nmid b_0$.
בנוסף: $p\nmid a_n=b_mc_k$, $p\nmid b_m$, $p\nmid c_k$.
יהי c_r המקדם הראשון שאינו מתחלק ב-p (כך ש-$p\mid c_0, p\mid c_1,\ldots,p\mid c_{r-1}$). r קיים כי $p\nmid c_k$). $0<r\le n$.
אם $r<n$, אז $p\mid a_r$ ובנוסף: $b_0c_r=\underset{\ddot{p}}{a_r}-(b_1\underset{\ddot{p}}{c_{r-1}}+\ldots+b_r\underset{\ddot{p}}{c_0})$
לכן $p\mid b_0c_r$, סתירה כי $p\nmid b_0$, $p\nmid c_r$.
לומר $r=n$. $\deg f\le\deg h$. סתירה. f אי-פריק. □

דוגמאות: 1) $f(x)=x^5-4x+2$ אי פריק: $p=2$.
2) יהי p ראשוני. נסמן: $\Phi_p(x)=\frac{x^{p-1}}{x-1}=\sum_{i=0}^{p-1}x^i$ (הפולינום הציקלוטומי)
נראה כי $\Phi_p(x)$ הינו אי-פריק מעל $\mathbb{Q}$. קל לראות שקריטריון אייזנשטיין מתקיים עבור $f=\Phi_p(x+1)$. אזי f אי פריק לכן $\Phi_p(x)$ אי פריק.

טענה $f(x)$ אי פריק מעל $\mathbb{Q}$ $\Leftrightarrow$ $f(\varphi(x))$ אי פריק מעל $\mathbb{Q}$, כאשר $\varphi(x)$ איזומורפיזם. לדוג': $f(x)$ אי פריק מעל $\mathbb{Q}$ $\Leftrightarrow$ $f(x+c)$ אי פריק מעל $\mathbb{Q}$.

הרחבה של שדות

הגדרה יהיו F ו-L שדות. נאמר כי L **הרחבה** של F אם קיים הומומורפיזם של חוגים $\varphi:F\to L$. נסמן זאת: $F\subset L$.

הגדרה תהי L הרחבה של F. איבר $\alpha\in L$ יקרא **אלגברי** מעל F אם קיים פולינום $f\in F[x]$ כך ש-$f(\alpha)=0$. אם α אינו אלגברי מעל F נאמר כי הוא **טרנסצנדנטי**.

למה: נניח כי $\alpha\in L$ אלגברי מעל $\mathbb{F}$, כאשר L הרחבה של $\mathbb{F}$. אז קיים פולינום מתוקן יחיד $p\in\mathbb{F}[x]$ המקיים: 1) $p(\alpha)=0$.

2) לכל $f\in\mathbb{F}[x]$ כך ש- $f(\alpha)=0$ מתקיים $p|f$.

הוכחה: ניקח את הפולינום ב- $\mathbb{F}[x]$ עם הדרגה המינימלית כך ש-$L\ni\alpha$ שורש שלו (קיים כזה, כי α אלגברי), נסמנו $p(x)$. בלי הגבלת הכלליות, $p(x)$ מתוקן (ע"י כפל בסקלר).
יהי $f(x)\in\mathbb{F}[x]$ פולינום כך ש- $f(\alpha)=0$. מאלגוריתם החלוקה נובע כי קיימים r,q ב- $\mathbb{F}[x]$, כך ש- $f(x)=p(x)q(x)+r(x)$, כאשר $r(x)=0$ או $\deg r<\deg p$.
נציב α ונקבל $r(\alpha)=0$. ממינימליות p, $r\equiv0$ $\Leftarrow$ $f(x)=p(x)q(x)$ $\Leftarrow$ $p|f$ כדרוש.
- נותר להראות את יחידות p. אם גם $\tilde{p}$ מקיים את 1), 2) אז:
$p|\tilde{p}$ ו- $\tilde{p}|p$, וכיוון ששניהם מתוקנים: $p=\tilde{p}$. □

הגדרה: יהי $\alpha\in L$ אלגברי מעל $\mathbb{F}$, כאשר L הרחבה של $\mathbb{F}$. הפולינום שאת קיומו הוכחנו בלמה האחרונה נקרא **הפולינום המינימלי** של α מעל $\mathbb{F}$.

מסקנה: הפולינום המינימלי של $\alpha\in L$ אי-פריק מעל $\mathbb{F}$.

דוגמה: - הפולינום המינימלי של $\sqrt{2}$ מעל $\mathbb{Q}$ הינו x^2-2
- נסמן $p(x)=x^4-10x+1$. נראה כי $p(x)$ אי-פריק מעל $\mathbb{Q}$, מתקיים:

$$p(x)=(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3})$$

לכן: $p(\sqrt{2}+\sqrt{3})=0$. קל לראות כי הפולינום $p(x)$ מינימלי עבור $\sqrt{2}+\sqrt{3}$.
- $\zeta_n=e^{\frac{2\pi i}{n}}$ הינו אלגברי מעל $\mathbb{Q}$ כי הוא שורש של x^n-1. הפולינום המינימלי של ζ_n מעל $\mathbb{Q}$ נקרא **הפולינום הציקלוטומי** ה-n-י ומסומן $\Phi_n(x)$. דרגתו היא $\varphi(n)$, כאשר φ פונקציית אוילר. אם $n=p$ ראשוני $\Phi_p(x)=\sum_{i=0}^{p-1}x^i$.

הגדרה: נניח כי $\mathbb{F}\subset L$ הרחבה של שדות, ויהיו $\alpha_1,\dots,\alpha_n\in L$. נסמן:

$$\underline{\underline{\mathbb{F}[\alpha_1,\dots,\alpha_n]}}=\{h(\alpha_1,\dots,\alpha_n):h\in\mathbb{F}[x_1,\dots,x_n]\}\subseteq L$$

קל לבדוק ש- $\mathbb{F}[\alpha_1,\dots,\alpha_n]$ חוג. נסמן בנוסף:

$$\underline{\underline{\mathbb{F}(\alpha_1,\dots,\alpha_n)}}=\left\{\frac{\alpha}{\beta}:\alpha,\beta\in\mathbb{F}[\alpha_1,\dots,\alpha_n],\ \beta\neq0\right\}\subseteq L$$

קל לבדוק כי $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ שדה. ↙ חלוקה בשדה.

למה: $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ הינו תת שדה הקטן ביותר ב- L המכיל את $\mathbb{F}$ ואת $\alpha_1,\dots,\alpha_n$.

הוכחה: כל תת שדה K של L המכיל את $\mathbb{F}$ ואת $\alpha_1,\dots,\alpha_n$ חייב להכיל גם (מסגירות לכפל, חיבור והופכי) את $\frac{p(\alpha_1,\dots,\alpha_n)}{q(\alpha_1,\dots,\alpha_n)}$ כאשר $p,q\in\mathbb{F}[x_1,\dots,x_n]$ ו- $q(\alpha_1,\dots,\alpha_n)\neq0$. □

הערה: קיבלנו: $\mathbb{F}\subseteq\mathbb{F}(\alpha_1,\dots,\alpha_n)\subset L$. נאמר) כי $\mathbb{F}(\alpha_1,\dots,\alpha_n)$ מתקבל מ- $\mathbb{F}$ ע"י צירוף $\alpha_1,\dots,\alpha_n$.

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 $\mathbb{F}$ 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! (בתנאי 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 $\varphi(f)=f(\alpha)=0$ $\therefore$ מלמה שהוכחנו, $p\mid f$ (p מינימלי של α) ולכן $f=pg$ 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: נשים לב כי כל הומומורפיזם מ- $\mathbb{F}[\alpha]$ נקבע באופן יחיד ע"י הערכים של α ואיברי $\mathbb{F}$. □

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 $f(x)$, וכן $\gcd(r,s)=1$.
אז $r\mid a_0$ ו- $s\mid a_n$.

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

פתרון: ראינו שהפולינום מתוקן, אם יש לו שורש רציונלי אז הוא שלם.
קל לראות כי $1,2,3$ לא שורשים ו- $x^4-10x^2+1>0$ עבור $x\geq 4$.
אז אין לו שורשים ב- $\mathbb{Q}$. נניח כי: $(x^2+ax+b)(x^2+cx+d)=x^4-10x^2+1$.
בהשוואת מקדם x^3 נקבל: $a=-c$. $(x^4-10x^2+1)=(x^2+ax+b)(x^2-ax+c)$
מקדם חופשי: $bc=1$. מקדם של x^2: $b+c-a^2=-10$. x: $ac=ab$.