תרגיל מספר 10 מבנים אלגבריים

1. יהי R חוג, ונניח שקיימים $a, b \in R$ איברים נילפוטנטיים. הוכיחו או הפריכו:
   (א) $a+b$ נילפוטנטי.
   (ב) ab נילפוטנטי.
   (ג) שני הסעיפים הקודמים עם R קומוטטיבי.

2. מצאו חוג R עבורו הקבוצות הבאות **אינן** תת־חוג:
   (א) $S \subseteq R$ אוסף האיברים שאינם הפיכים.
   (ב) $S \subseteq R$ אוסף האיברים הנילפוטנטיים.

3. יהא $0 \neq f(x) \in \mathbb{F}[x]$ פולינום מדרגה n. ראינו בתירגול כי ${}^{\mathbb{F}[x]}/_{I(f)} = \{[g]|\ \deg(g) < n\ g \in {}^{\mathbb{F}[x]}/_{\langle f \rangle}\}$. הוכיחו כי בקבוצה זאת האיברים שונים. כלומר, יהיו g_1, g_2 שני פולינומים מדרגה קטנה מ n. הוכיחו כי

$$[g_1] = [g_2] \iff g_1 = g_2$$

(להזכירכם היחס השקילות הוא $g \sim_I g' \iff g - g' \in I$).

4. עבור הפולינומים $a(x) = 1 + 2x^2, b(x) = 2 + x \in \mathbb{R}[x]$ מתקיים כי $1 = \gcd(a, b)$ ומתקיים

$$1 = \frac{1}{9}a(x) - \frac{2x-4}{9}b(x)$$

מצאו פולינום $f(x)$ המקיים

$$f(x) \quad \sim_{a(x)} \quad 5$$

$$f(x) \quad \sim_{b(x)} \quad x$$

כאשר $g \sim_{a(x)} f$ פירושו $g \sim_{I(a(x))} f$ או יותר מפורש $f - g \in I(a(x))$. [השתמשו ברעיון דומה למשפט השאריות הסיני]

5. תזכורת: יהיו R_1, R_2 חוגים. פונקציה $\phi : R_1 \to R_2$ תקרא הומומורפיזם של חוגים אם
   1. לכל $x, y \in R_1$ מתקיים $\phi(xy) = \phi(x)\phi(y)$
   2. לכל $x, y \in R_1$ מתקיים $\phi(x+y) = \phi(x) + \phi(y)$

הערה: נסמן $R_1 \cong R_2$ (R_1 איזומורפי ל R_2) אם קיים $\phi : R_1 \to R_2$ הומורפזים חח"ע ועל.

(א) הוכיחו כי הגרעין $\ker\phi = \{x \in R_1 |\, \phi(x) = 0\}$ הוא אידיאל של R_1.

(ב) הוכיחו כי $Im(\phi) = \{\phi(x) |\, x \in R_1\}$ הוא תת חוג של R_2 (כלומר הוא חוג ביחס לפעולות של R_2).

6. משפט האיזומורפיזם הראשון לחוגים: יהיו R_1, R_2 חוגים ויהא $\phi : R_1 \to R_2$ הומומורפיזם של חוגים אזי $R_1/\ker\phi \cong Im(R_2)$.

(א) יהא $\mathbb{F}$ שדה, $\mathbb{K} \subseteq \mathbb{F}$ תת שדה שלו ו $a \in \mathbb{F}$. נגדיר $\phi : \mathbb{K}[x] \to \mathbb{F}$ ע"י $\phi(f) = f(a)$ (פונקציה זאת נקראת הומומורפיזם ההצבה). הוכיחו כי ϕ הומומורפיזם.

(ב) נתסכל על הומומורפיזם ההצבה הבא: $\phi; \mathbb{Q}[x] \to \mathbb{R}$ המוגדר ע"י $\phi(f) = f(\sqrt{2})$ (שימו לב שזה דוגמא לסעיף הקודם). הוכיחו כי $Im(\phi) = \mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} |\, a, b \in \mathbb{Q}\right\}$ ומצאו $\hat{f}(x) \in \mathbb{Q}[x]$ כך ש $\mathbb{Q}[x]/I(\hat{f}) \cong \mathbb{Q}[\sqrt{2}]$

.7

(א) הוכיחו כי $f(x) = x^2 + x + 4 \in \mathbb{Z}_{11}[x]$ ראשוני ולכן $\mathbb{F} = \mathbb{Z}_{11}[x]/\left\langle x^2 + x + 4\right\rangle$ שדה.

(ב) מצאו $[3x + 2]^{-1}$ ב $\mathbb{F}$ הנ"ל.

8. יהי $\mathbb{F} = \mathbb{F}_{2^n}$ שדה סופי הוא מקיים כי $1 + 1 = 0$. הוכיחו כי כל איבר בו הוא ריבוע כלומר $\forall x \in \mathbb{F} \exists y \in \mathbb{F} :\ x = y^2$.
הדרכה: נגדיר העתקה : $\phi : \mathbb{F} \to \mathbb{F}$ ע"י $\phi(x) = x^2$ הראו שהעתקה זו היא חח"ע והסיקו כי ϕ על ולכן הטענה מתקיימת.

9. יהא $\mathbb{F} = \mathbb{F}_{p^n}$ שדה עם p^n איברים. הוכיחו כי

$$x^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}^\times} (x - \alpha)$$

כאשר השיוון הוא שיוון פולינומים ו $\mathbb{F}^\times = \mathbb{F} \backslash \{0\}$.
הסיקו את משפט וילסון: יהא p מספר ראשוני אי זוגי אזי

$$(p-1)! \equiv -1 \mod p$$