תורת החוגים:

תזכורת:

מבנה אלגברי: קבוצה A עם פעולה * שמקיימת סגירות: $a,b \in A \Leftarrow a*b \in A$.

אגודה: מבנה אלגברי עם חוק הקיבוץ: $a*(b*c) = (a*b)*c$.

מונויד: אגודה עם איבר יחידה (e).

חבורה: מונויד עם הופכי לכל איבר שונה מ-0.

חבורה אבלית: לכל g,h מתקיים: $g*h = h*g$.

הגדרה: חוג הוא מבנה אלגברי R עם 2 פעולות *, + כך ש:
1. (+, R) חבורה אבלית.
2. (*, R) אגודה.
3. מתקיים חוק הפילוג: $r(a+b) = ra+rb,\ (a+b)r = ar+br$

- אם פעולת הכפל חילופית אזי R חוג קומוטטיבי.
- אם $(R, *)$ מונויד אז R חוג עם יחידה.
- אם $R^* = (R\backslash\{0\}, *)$ חבורה אז R הוא חוג עם חילוק.

הגדרה: אם R חוג ו-G חבורה אזי חוג החבורה **RG**:
$RG = \{\sum_{g\varepsilon G} a_g g \mid a_g \varepsilon R\}$ ונגדיר את הפעולות +, * כך:

$$\sum_{g\varepsilon G} a_g g + \sum_{g\varepsilon G} b_g g = \sum_{g\varepsilon G} (a_g + b_g) g$$

$$\sum_{g\varepsilon G} a_g g * \sum_{h\varepsilon G} b_h h = \sum_{g,h\varepsilon G} a_g b_h gh$$

אם G לא אבלית ← RG אינו קומוטטיבי.

הגדרה: חוג קומוטטיבי R כך ש-$(R\text{-}\{0\}, *)$ חבורה נקרא שדה.

משפט: $\mathbf{Z}_n$ שדה $\Leftrightarrow$ n ראשוני.

משפט: תכונות כלליות של חוג:

אם R חוג, $a,b \in R$, אזי:
1. $a*0 = 0*a = 0$.
2. $a(-b) = (-a)b = -ab$.
3. $(-a)(-b) = ab$.

הגדרה: תת-חוג S של חוג R, $S \le R$, הוא תת-קבוצה $S \subseteq R$ כך ש:
1. $(S, +)$ תת-חבורה של $(R, +)$.
2. $(S, *)$ תת-אגודה של $(R, *)$.

תוצאה: $S \le R \Leftrightarrow S \neq \phi$ ולכל $a,b \in S$ אז $a\text{-}b,\ ab \in S$.

אידיאלים:

הגדרה: אידיאל שמאלי (ימני) הוא תת-חבורה $I \le R$ כך שלכל $r \in R$ ו-$a \in I$: $ra \in I$ ($ar \in I$).

הגדרה: אידיאל I בחוג R הוא תת-חוג $I \le R$ כך ש-I אידיאל שמאלי וימני, כלומר לכל $r \in R$ ו-$a \in I$: $ra, ar \in I$.

לכל חוג יש 2 אידיאלים טריוויאליים: החוג עצמו ו- $I = \{0\}$.

הגדרה: חוג שאין בו אידיאלים (דו-צדדיים) פרט ל-$\{0\}$ ולעצמו נקרא חוג פשוט.

עובדה: אם F שדה אזי $M_n(F)$ הוא חוג פשוט.

הגדרה: בחוג קומוטטיבי R כל $a \in R$ מייצג אידיאל: $I = (a) = \{ra \mid ar \in R\}$ והוא נקרא אידיאל ראשי.

טענה: אם $1 \in I$ (I אידיאל) $\Leftarrow I = R$.

מסקנה: אין אידיאל לא טריוויאלי שמכיל את איבר היחידה.

הגדרה: הומומורפיזם $f: S \to R$ מחוג S לחוג R הוא ההעתקה שמקיימת:
1. $a,b \in S$: $f(a+b) = f(a) + f(b)$.
2. $a,b \in S$: $f(ab) = f(a)f(b)$.
3. מעבירה איבר יחידה לאיבר יחידה: $f(1_S) = 1_R$.

<u>תוצאה:</u> נניח ש: f: S → R הומומורפיזם של חוגים אזי:
1. **Im(f)** תת-חוג של **R**.
2. **Ker(f)** אידיאל ב-**S**.

<u>הגדרה:</u> אם R חוג ו-$I \triangleright R$ אז <u>חוג המנה</u> R/I הוא: $R/I = \{a+I \mid a\varepsilon R\}$, כאשר הפעולות הן: (a+I)(b+I) = ab + I, (a+I)+(b+I) = (a+b) + I .

<u>טענה:</u> חוג מנה של חוג קומוטטיבי הוא קומוטטיבי.

<u>משפט האיזומורפיזם ה-1:</u> אם f: S → R אפימורפיזם של חוגים (הומומורפיזם + על) אזי:

$$S/\ker(f) \cong R$$

<u>טענה:</u> $\ker(f) \triangleright R$

<u>טענה:</u> אם g(w) ϵ F[w] אזי: g(0) = 0 ⟺ g(w) = w*k(w), כאשר k(w) ϵ F[w].

למשל: w = x-3: (x-3)k(x-3) = g(w) = wk(w) . ואם נגדיר הומומורפיזם $\phi_a : F[x] \to F$ אזי $\ker(\phi_3) = \{(x-3)h(x) \mid h(x) \in F[x]\}$ = האידיאל הראשי שנוצר ע"י x-3, ולפי משפט האיזומורפיזם ה-1: $F[x]/(x-a)F[x] \cong F$

<u>פעולות של אידיאלים:</u>

$I,J \triangleright R$

$$I \cap J = \{a \in R \mid a \in I, a \in J\}, (a)\cap(b) = (d), d = [a,b]$$
$$I + J = \{a+b \mid a \in I, b \in J\}, (a)+(b) = (d), d = (a,b)$$
$$IJ = \{\sum a_i b_i \mid a_i \in I, b_i \in J\}, (a)(b) = (ab)$$

כלומר, מכפלה של אידיאלים ראשיים הוא האידיאל הראשי הנוצר ע"י מכפלת היוצרים

בד"כ: $IJ \subseteq I \cap J \subseteq I + J$.
- הכלה ממש מתקיימת כאשר $(a_i, a_j) \neq 1$
- אם I = J אזי
- <u>טענה:</u> אם R חוג קומוטטיבי עם יחידה ו-I + J = R אזי $IJ = I \cap J$.

<u>הגדרה:</u> אידיאל $P \neq R$ בחוג R הוא <u>ראשוני</u> אם לכל a,b ϵ R, ab ϵ P ⟸ a ϵ P או b ϵ P.
<u>הגדרה:</u> <u>מקסימלי</u> אם לא קיים אידיאל I כך ש-
<u>משפט:</u> כל אידיאל מקסימלי בחוג קומוטטיבי עם יחידה הוא ראשוני.
(אולם, ראשוני ⟸ מקסימלי, למשל: 0Z ראשוני ואינו מקסימלי כי: $0Z \subseteq 3Z \subseteq Z$).
<u>טענה:</u> אם $I \triangleright R$, I = (a) ו-a הפיך אזי I = R.

<u>הגדרה:</u> <u>סכום ישר</u> של חוגים R, S הוא: $R \oplus S = \{(r,s) \mid r \in R, s \in S\}$, כאשר החיבור והכפל הוא לפי מרכיבים: (r, s) + (r', s') = (r + r', s + s') (r, s)(r', s') = (rr', ss').
<u>משפט השארית הסיני:</u> אם $I,J \triangleright R$ כאשר I + J = R, R חוג קומוטטיבי עם יחידה אזי:

$$R/I\cap J = R/I \oplus R/J$$

<u>למה:</u> בחוק עם חילוק (ובפרט בשדה) R אין אידיאלים פרט ל-{0}, R.
<a> = {האידיאל הקטן ביותר שמכיל את a}

כאשר R חוג כללי: $\langle a \rangle = \{na, r_1 a, a r_2, r_3 a r_4 \mid n \in Z, r_i \in R\}$

אם R קומוטטיבי: $(a) = \{na + r_1 a + a r_2 + r_3 a r_4 \mid n \in Z, r_i \in R\}$

$(a) = \{na + ra \mid n \in Z, r \in R\}$

אם R חוג עם יחידה: $(a) = \{r_1 a r_2 \mid n \in Z, r_i \in R\}$

אם R חוג קומוטטיבי עם יחידה: אידיאל ראשי - $(a) = \{ra \mid r \in R\} = Ra$

<u>הגדרה:</u> <u>תחום שלמות</u> הוא חוג קומוטטיבי שבו ab = 0 ⟸ a = 0 או b = 0.
<u>הגדרה:</u> איבר $0 \neq a \in R$ נקרא מחלק 0 אם קיים $0 \neq b \in R$ כך ש-ab = 0 או ba = 0.
<u>מסקנה:</u> בתחום שלמות אין מחלקי 0.

<u>משפט:</u> תחום שלמות סופי הוא שדה.
<u>משפט:</u> נניח ש-R חוג קומוטטיבי עם יחידה אזי $P \triangleright R$ ראשוני $\Leftrightarrow$ R/P תחום שלמות.
<u>משפט:</u> נניח ש-R חוג קומוטטיבי עם יחידה אזי $M \triangleright R$ מקסימלי $\Leftrightarrow$ R/M שדה.
<u>טענה:</u> אם R חוג קומוטטיבי עם יחידה אזי S תחום שלמות $\Leftrightarrow$ $\{0\} \triangleright S$ אידיאל ראשוני.
<u>טענה:</u> I מקסימלי $\Leftarrow$ I ראשוני.

<u>משפט:</u> לכל תחום שלמות R אפשר לבנות <u>שדה שברים</u> בצורה:
$$Q = QF(R) = \{\frac{p}{q} \mid p \in R, q \in R^*, \frac{p}{q} = \frac{p'}{q'} \Leftrightarrow pq' = qp'\}$$
עם הפעולות: $\frac{p}{q} + \frac{r}{s} = \frac{ps+rq}{qs}, \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$
ואפשר לשכן את R ב-**Q** ע"י $R \to Q$
$$r \mapsto \frac{r}{1}$$

פריקות בחוגים:

<u>הגדרה:</u> R תחום שלמות. לכל a, b ∈ R נגדיר **<u>a | b</u>** אם קיים k ∈ R כך ש- b = ak.
<u>טענה:</u> a | b $\Leftrightarrow aR \supseteq bR$
<u>הגדרה:</u> R תחום שלמות. a,b ∈ R. נגיד ש-a, b <u>רעים</u> אם קיים איבר הפיך u כך ש- b = au, כלומר:
$$b \mid a \wedge a \mid b \Leftrightarrow a \sim b$$
<u>טענה:</u> a ~ b הוא יחס שקילות (רפלקסיבי: a ~ a, טרנזיטיבי: b ~ c, a ~ b $\Leftarrow$ a ~ c,
סימטרי: a ~ b $\Leftrightarrow$ b ~ a).
<u>טענה:</u> כל איבר הפיך u הוא רע של 1: 1 ~ u.
<u>טענה:</u> h(x) הפיך $\Leftrightarrow$ h(x) = c ∈ F ו-c הפיך.
<u>טענה:</u> a ~ b $\Leftrightarrow$ ל-a ול-b יש אותם מחלקים.
<u>טענה:</u> a ~ b $\Leftrightarrow$ aR = bR.
<u>הגדרה:</u> איבר p ∈ R לא הפיך בתחום שלמות R נקרא <u>ראשוני</u> אם p | bc $\Leftarrow$ p | b או p | c.
<u>הגדרה שקולה:</u> איבר p ∈ R לא הפיך בתחום שלמות R נקרא <u>ראשוני</u> אם <a> ראשוני.
<u>הגדרה:</u> איבר $0 \neq q \in R$ לא הפיך בתחום שלמות R <u>אי-פריק</u> אם q = bc $\Leftarrow$ b הפיך או c הפיך,
ז"א: המחלקים היחידים של q הם איברים הפיכים או רעים של q.
<u>הגדרה שקולה:</u> איבר $0 \neq q \in R$ <u>אי-פריק</u> אם הוא לא הפיך ואין לו מחלקים אמיתיים.
<u>תוצאה:</u> איבר a <u>פריק</u> אם a = bc ו-b, c שניהם אינם הפיכים.
<u>משפט:</u> כל איבר ראשוני הוא אי-פריק, אבל p אי פריק $\not\Leftarrow$ p ראשוני.

<u>הגדרה:</u> <u>תחום גאוס</u> הוא תחום שלמות R שבו לכל איבר $a \neq 0$ ולא הפיך קיים פירוק לאי-פריקים:
$a = p_1 p_2 \cdots p_n$ והוא יחיד עד כדי תמורה של הגורמים והצבת רעים.
<u>משפט:</u> בתחום גאוס: p ראשוני $\Leftrightarrow$ p אי-פריק.
<u>הגדרה:</u> <u>תחום ראשי</u> הוא תחום שלמות שבו כל אידיאל הוא ראשי.
<u>משפט:</u> בתחום ראשי I ראשוני $\Leftrightarrow$ I מקסימלי.
<u>טענה:</u> אם R תחום ראשי, a,b ∈ R אזי gcd(a,b) הוא יוצר של האידיאל (a) + (b) = {as + bt | s,t ∈ R}
ו-[a,b] היוצר של $(a) \cap (b)$.
<u>משפט:</u> R תחום ראשי $\Leftarrow$ R תחום גאוס.
<u>משפט:</u> בתחום ראשי R, אידיאל שנוצר ע"י איבר אי-פריק הוא מקסימלי.
<u>מסקנה:</u> בתחום ראשי, איבר אי-פריק הוא ראשוני.

<u>הגדרה:</u> <u>נורמה:</u> $N : R \to \mathbf{N} \cup \{0\}$ שמקיימת:
1. N(d) = 0 $\Leftrightarrow$ d = 0.
2. N(ab) = N(a)N(b).

<u>הגדרה:</u> <u>תחום אוקלידי</u> הוא תחום שלמות E שבו יש פונקציה $d : E \to \mathbf{Z} \cup \{-\infty\}$ כך ש:
1. אם $b \neq 0$ אז $d(ab) \geq d(a)$
2. לכל a,b ∈ E, $b \neq 0$, קיימים q, r ∈ E כך ש- d(r) < d(b), a = qb + r.
<u>משפט:</u> F[x] הוא תחום אוקלידי (deg(0) = - ∞).

עובדה: ב-Z[i] יש 4 הפיכים $\pm 1, \pm i$ $\Leftarrow$ לכל איבר יש 4 רעים.
משפט: תחום אוקלידי הוא תחום ראשי.
למה: נניח ש-Z ∋ n, m, $m \neq 0$, אזי קיימים q', r' כך ש-n = q'm + r', $-\frac{1}{2}|m| < r' \leq \frac{1}{2}|m|$
דוגמה:

כללים של תחום אוקלידי:
משפט: E תחום אוקלידי. a, b ∈ E. a ~ b $\Leftarrow$ d(a) = d(b).
טענה: d(a) = d(b) $\not\Leftarrow$ a ~ b.
טענה: אם F שדה אז ההפיכים ב-F[x] הם האיברים של F - {0}.
משפט: u הפיך $\Leftrightarrow$ d(u) = d(1).
משפט: $a,b \neq 0$, b$\not\sim$1 $\Leftarrow$ d(ab) > d(a).
למה: d(0) > d(1).
טענה: אם עבור a, b ∈ E מתקיים d(ab) < d(a) אז ab = 0 $\Leftarrow$ b = 0.
טענה: לכל $0 \neq a \in R$ אם d(ab) = d(a) $\Leftarrow$ b הפיך.
טענה: אם $a \neq 0$ אזי $d(a) \geq d(1)$.
טענה: d(a) = d(0) $\Leftrightarrow$ a = 0.
כלל:

כלל: מס' המחלקים של מס' (עד כדי רעים) z: $z = p_1^{a_1} \cdots p_n^{a_n}$ הוא $t(z) = (a_1 + 1)\cdots(a_n + 1)$
טענה: אם E תחום אוקלידי, z ∈ E, a הפיך, $z = ap_1^{a_1} \cdots p_n^{a_n}$, $i \neq j \Rightarrow p_i \neq p_j$ אז מס' האידיאלים (r) כך ש- $(z) \subseteq (r)$ הוא $t(z) = (a_1 + 1)\cdots(a_n + 1)$.
כלל: מס' האידיאלים ב- R/I הוא מס' האידיאלים ב-R שמכילים את I.

דוגמה:

איברים אי פריקים ב-Z[i]:
טענה: נניח ש-a + bi אי פריק. $d(a+bi) = \begin{cases} p \\ p^2 \end{cases}$, Z ∋ p ראשוני.
תת-טענה: a + bi אי-פריק $\Leftrightarrow$ a - bi אי-פריק.
תת-טענה: a + bi הפיך $\Leftrightarrow$ a - bi הפיך.
משפט: האיברים האי-פריקים ב-Z[i] הם:
1. מס' ראשוניים Z ∋ p כך ש-p = 3mod4 (או הרעים).
2. איברים a + bi כך ש- $p = a^2 + b^2 \equiv 1 \bmod 4, 2 \bmod 4$, p ראשוני.

משפט: כל מס' ממשי n = 1mod4 הוא סכום של 2 ריבועים $(a^2 + b^2)$.

איברים אי-פריקים כדוגמאות לתחום אוקלידי:
1. E = **Z**, d(n) = |n|. האיברים האי-פריקים הם: $\pm p$, p ראשוני.
2. **Z**[i]. האיברים האי-פריקים הם:
א. $\pm p, \pm ip$, p ראשוני ב-**Z** ו-p = 3mod4.
ב. $\pm(1+i), \pm(1-i) = \pm i(1+i)$.
ג. לכל ראשוני p = 1mod4: $\pm i(c-di), \pm 1(c-di), \pm i(c+di), \pm 1(c+di)$

דוגמה:

פירוק ב-Z[i]:
1. חישוב $d(z) = z\bar{z}$.
2. פירוק d(z) לגורמים ראשוניים.
3. פירוק הראשונים ל-p = (c + di)(c - di).
4. לבדוק איזה מהאי-פריקים מחלק את z_0.
5. את המחלק המשותף של a, b לפרק לגורמים ב-**Z**[i].
6. לאסוף ביחד את הרעים של אותו פירוק.

דוגמה:

פירוק פולינומים:
- אם <u>deg f(x) = 0</u> ⇐ f(x) = c (כלומר c = 0 או c הפיך) ולכן לא אי-פריק.
- אם <u>deg f(x) = 1</u> - כל פולינום מדרגה 1 הוא אי-פריק.
- אם <u>deg f(x) = 2, 3</u>: f(x) אי-פריק⟺ אין איבר a ϵ F כך ש-f(a) = 0.

טענה: $f(x) = a_0 + \ldots + a_n x^n$, $\forall i, a_i \in \mathbf{Z}, a_n \neq 0, n > 1$, יהיו k,l ϵ **Z**, (k, l) = 1. אם $\frac{k}{l} \in \mathbf{Q}$ שורש של f אזי $l \mid a_n, k \mid a_0$.

טענה: אם לפולינום אין שורשים ב-$\mathbf{Z}_2$ אז אין לו שורשים ב-**Z**.

טענה: f(x) אי פריק ב-F[x] כאשר f(x) = g(x)h(x) ⇐ g(x) הפיך או h(x) הפיך.

טענה שקולה: f(x) אי פריק אם f(x) אינו הפיך ואין לו פירוק שונה מהטריוויאלי, כלומר אם f(x) = g(x)h(x) אזי f(x) ~ g(x) או f(x) ~ h(x).

הקריטריון של אייזנשטיין: אם f(x) פולינום ב-**Z**[x] כך ש- $f(x) = a_0 + \ldots + a_n x^n$ וקיים p כך ש-$p \nmid a_n$, $p \mid a_{n-1}, a_{n-2}, \ldots, a_0$, $p^2 \nmid a_0$ אז f(x) אי-פריק ב-**Z**[x] וב-**Q**[x].

טענה: f(x) אי פריק מעל **Q** ⟺ f(x + c) אי פריק מעל **Q**, c קבוע.

שדות:

- F שדה ולכן מכיל את 1. $g: \mathbf{Z} \to F$, $n \mapsto n \cdot 1$:

$\mathrm{Im}(g) \le F$ ומכיל את 1.

לפי משפט האיזומורפיזם ה-1: $\mathrm{Im}(g) \cong \mathbf{Z}/\ker(g)$.

כיוון שבשדה אין מחלקי 0 ⇐ גם ב-Im(g) אין מחלקי 0 ⇐ $\mathbf{Z}/\ker(g)$ תחום שלמות

⇐ ker(g) אידיאל ראשוני, לכן: $\ker(g) = \begin{cases} (p) \\ \{0\} = (0) \end{cases}$

המס' 0 או p שיוצר את ker(g) נקרא <u>אפיון</u> של F.

טענה: בכל שדה יש <u>שדה ראשוני</u> שהוא $\mathbf{Z}/p\mathbf{Z}$ במקרה של אפיון p או **Q** במקרה של אפיון 0.

למה: נניח ש-F, K שדות ו-$F \le K$. אם F תת-שדה של K אזי <u>K מרחב-וקטורי מעל F</u>, כלומר:
1. (K, +) חבורה אבלית.
2. הפעולה של מכפלה באיבר מ-F מקיימת את התנאים הבאים עבור c,d ϵ K, a,b ϵ F:
   א. (a + b)c = ac + bc.
   ב. a(c + d) = ac + ad.
   ג. (ab)c = a(bc).
   ד. 1*c = c.

הגדרה: אם $F \le K$, F, K שדות, אז <u>המימד של K מעל F</u> (=העוצמה של הבסיס של K מעל F) נקרא <u>הדרגה של K מעל F</u> ומסומן: $[K : F] = \dim_F K$

למה: חיתוך של שדות הוא שדה.

איברים אלגברים ואיברים נעלים:

הגדרה: יהי K שדה, $F \le K$ תת-שדה. נניח ש-$a_1, \ldots, a_n$ ϵ K. נגדיר את <u>השדה שנוצר מעל F ע"י $a_1, \ldots, a_n$</u> להיות: $F(a_1, \ldots, a_n) = \bigcap_{\substack{F_i \le K \\ \{a_1, \ldots, a_n\} \subseteq F_i}} F_i$

דוגמה: K = **C**, F = **Q**, a = i, n = 1: **Q**(i) = {a + bi | a, b ϵ **Q**}.

<u>הגדרה:</u> יהי K שדה, $F \le K$ תת-שדה, $a \in K$:
א. אם קיים פולינום $f(x) \in F[x]$ כך ש-$f(a) = 0$ אז a <u>אלגברי</u> מעל F.
ב. אם אין פולינום כנ"ל אזי a <u>נעלה.</u>
ג. אם a אלגברי ו-$f(x)$ פולינום מדרגה מינימלית כך ש-$f(a) = 0$ אז $f(x)$ נקרא <u>הפולינום המינימלי</u> של a.

<u>משפט:</u> יהי K שדה, $F \le K$ תת-שדה, $a \in K$ אלגברי ו-$f(x) \in F[x]$ הפולינום המינימלי של a, אזי:
1. הפולינום $f(x)$ אי-פריק בתחום האוקלידי $F[x]$.
2. השדה המינימלי $F(a)$ הוא:

$$F(a) = \{b_0 + b_1 a + ... + b_{n-1} a^{n-1} \mid b_i \in F, i = 0,...,n-1, n = \deg f(x)$$

3. $F[x] \big/ (f(x)) \cong F[a]$

<u>מסקנה:</u> $[\,F[a] : F\,] = n$.

<u>דוגמה:</u>

<u>טענה:</u> $F[a]$ הנ"ל הוא שדה ו-$F(a) = F[a]$.

<u>משפט:</u> אם K שדה, $F \le K$ תת-שדה, $a \in K$ נעלה מעל F אזי $F[x] \cong F(a)$, כאשר:
שדה השברים של $F[x]$ = $F(x) = \{\frac{g(x)}{h(x)} \mid h(x) \neq 0\}$

<u>הגדרה:</u> שדה המרוכבים אינו ניתן להרחבה והוא נקרא <u>סגור אלגברית.</u>

<u>הגדרה:</u> <u>אלגברה</u> = חוג + מרחב וקטורי, למשל: $\mathbf{Q}(\sqrt{2})$ הוא שדה ומרחב וקטורי שבסיסו $\{1, \sqrt{2}\}$
לכל מרחב וקטורי יש מימד.

<u>מימד ההרחבה = מעלת הפולינום האי-פריק</u>, למשל: מימד ההרחבה של $x^2 - 2$ מעל $\mathbf{Q}$ = **2** =
המימד של $\mathbf{Q}(\sqrt{2})$ · $\mathbf{Q}[x] \big/ \langle x^2 - 2 \rangle \cong \mathbf{Q}(\sqrt{2})$

<u>הגדרה:</u> F, K שדות. K נקרא <u>הרחבה פשוטה</u> של F אם קיים $a \in K$ כך ש-$F(a) = K$.

<u>שדות פיצול:</u>

$F \le K$ ונתון פולינום $f(x) \in F[x]$. רוצים למצוא את תת-השדה הכי קטן של K בו $f(x)$ מתפרק לגמרי לגורמים לינאריים. תת-שדה זו הוא <u>שדה הפיצול</u> של $f(x)$.

<u>טענה:</u> כל פולינום עם מקדמים ממשיים מתפרק לגמרי ב-**C**.

<u>משפט:</u> $[E : L] = m$, $[L : F] = n$ $\Leftarrow$ $[E : F] = mn$ ($F \le L \le E$).

<u>הגדרה:</u> נניח ש-F שדה, $F \le E$ כך ש-$[E : F] = n < \infty$.
איבר $a \in E$ כך ש-$E = F[a]$ נקרא <u>פרימיטיבי</u> מעל F ואז $1, a, ..., a^{n-1}$ בסיס של E מעל F.

<u>משפט:</u> אם F ממאפיין 0 ז"א $\mathbf{Q} \le F$ אז לכל הרחבה סופית $F \le E$ ($[E : F] = n < \infty$), קיים איבר פרימיטיבי $a \in E$ כך ש-$E = F[a]$.

<u>מסקנה:</u> אם $E = F[a_1, ..., a_m]$ אז אפשר למצוא איבר פרימיטיב מהצורה $a = c_1 a_1 + ... c_m a_m$, $c_i \in F$.

<u>הגדרה:</u> יהי F שדה $f(x) \in F[x]$ מונית, $\deg f(x) = n$.
<u>שדה פיצול</u> של $f(x)$ מעל F הוא שדה E, $F \le E$, כך ש-$f(x) \in F[x] \subset E[x]$, $f(x)$ מתפרק לגמרי: $f(x) = (x - a_1) \cdots (x - a_n)$, ואין תת-שדה L, $F \le L \le E$, שבו $f(x)$ מתפרק לגמרי.

<u>למה:</u> נניח ש-F שדה ו-$g(x) \in F[x]$ פולינום אי-פריק מעל F. אז קיים שדה L, $F \le L$, כך של-$g(x)$ יש שורש a ב-$L[x]$, $L=F[a]$ ו-$g(x)$ מתפרק: $g(x) = (x-a)l(x)$.

<u>טענה:</u> בתחום אוקלידי $F[y]$, אידיאל I שנוצר ע"י פולינום אי-פריק $g(y)$ הוא מקסימלי.

<u>משפט:</u> <u>קיום שדה פיצול:</u> יהי F שדה, $f(x)$ פולינום ב-$F[x]$. אז קיים שדה פיצול E של $f(x)$ מעל F.

<u>משפט:</u> <u>יחידות של שדה פיצול:</u> כל שני שדות פיצול של $f(x)$ מעל F הם איזומורפיים.

שדות סופיים:

1. אם F שדה סופי אז קיים ראשוני p ומס' טבעי n כך שיש ל-F p^n איברים.
2. לכל n ו-p קיים שדה סופי בעל p^n איברים והוא יחיד עד כדי איזומורפיזם.
3. יש ל-F תת-שדה F_p מסדר p ו-F הוא שדה הפיצול של הפולינום $f(x)=x^{p^n}-x$ מעל F_p.
4. לכל טבעי d, $d \mid n$, קיים תת-שדה יחיד בעל p^d איברים ואין תתי-שדות אחרים ב-F.
5. השורשים של $f(x)=x^{p^n}-x$ הם כולם שונים והם כל האיברים ב-F.
6. הדרגות של כל הגורמים האי-פריקים של $f(x)$ מעל F_p הם מחלקים של n וכל פולינום אי-פריק $g(x)$ ב-$F_p[x]$ מדרגה d כך ש-$d \mid n$ הוא גורם אי-פריק של $f(x)=x^{p^n}-x$
7. החבורה הכפלית $(F - \{0\}, *)$ של F היא ציקלית. היוצר a של $F^* = F - \{0\}$ הוא שורש של פולינום מינימלי מדרגה n, $F = F_p[a]$.

__הגדרה:__ אם R הומומורפיזם: $\alpha : \mathbf{Z} \to R$, $n \mapsto n \cdot 1$, קיים מס' $m \geq 0$ כך ש-$Ker(\alpha) = (m)$. המס' m נקרא __המאפיין__ של R.

אם R תחום שלמות אז המאפיין m הוא ראשוני $(m*1 = 0)$.

אם R שדה אז $\alpha(\mathbf{Z})$ הוא תת-שדה איזומורפי ל- $\mathbf{Z}/p\mathbf{Z}$.

אם המאפיין הוא 0 אז השדה מכיל תת-שדה איזומורפי ל-$\mathbf{Q}$.

__למה:__ אם K שדה כלשהו ו-$f(x)$ פולינום מדרגה m אז אין יותר מ-m שורשים של $f(x)$ ב-K.

__למה:__ $x^m - 1 \mid x^n - 1 \Leftarrow m \mid n$

$x^m - 1 \nmid x^n - 1 \Leftarrow m \nmid n$

__תזכורת על מספרים מודולו n:__

ב-$(\mathbf{Z}/n\mathbf{Z},+)$ היוצרים הם כל המספרים k שהם זרים ל-n: $\phi(n) = \#\{k \mid (k,n) = 1\}$.

אם p ראשוני אזי: $\phi(p^n) = p^a - p^{a-1} = (p-1)p^{a-1}$

אם $ab \neq p^n$ אזי: $\phi(ab) = \phi(a)\phi(b)$

__משפט:__ חבורה כפלית של שדה סופי היא חבורה ציקלית מסדר $p^n - 1$.

__הגדרה:__ לכל $d \mid p^n - 1$ נגדיר: $N_d = \{b \in F^* \mid |b| = d\}$

$$F^* = \bigcup_{d|p^n-1} N_d \Rightarrow |F^*| = \sum_{d|p^n-1} |N_d|$$

אם $N_d \cap N_{d'} = \phi \Leftarrow d \neq d'$

__טענה:__ אם $|N_d| = \phi(d) \Leftarrow N_d \neq \phi$ [אם $|N_d| = 0 \Leftarrow N_d = \phi$].

__למה:__ אם m מס' שלם אז $\sum_{d|m} \phi(d) = m$

__משפט:__ $f(x) = x^{p^n} - x$ שווה למכפלת כל הפולינומים האי-פריקים מעל $\mathbf{Z}_p$ שמעלתם מחלקת את n.

__שדה סופי כשדה פיצול:__

__משפט:__ לכל ראשוני p ולכל $n \geq 1$ קיים שדה יחיד מסדר p^n והוא שדה פיצול של הפולינום $f(x) = x^{p^n} - 1$

__משפט:__ p ראשוני, $n \geq 1$. הפולינום $g(x)$ אי פריק מעל F_p ומחלק את $f(x) = x^p - x$ $\Leftrightarrow$ $deg(g(x)) = n$.

__משפט:__ לשדה K בעל p^n איברים יש תת-שדה L בעל p^m איברים אם"ם $m \mid n$.

__בניית שדה מסדר $n = p^m$:__ נחפש פולינום אי-פריק ממעלה m מעל $\mathbf{Z}_p[x]$ ואז: $F \cong \mathbf{Z}_p[x]/$

__איך למצוא פולינומים אי-פריקים מעל F_p?__

- פולינום מדרגה 2, 3 הוא פריק $\Leftrightarrow$ יש לו שורש [לכן נציב את איברי F_p בפולינום לראות אם יש שורש].
- אם דרגת הפולינום גדולה מ-3 אפשר לנסות לפרק את $f(y)$, $y = x^r$.

__משפט:__ אם $a \in F_p$ אז $a^p = a$.

$$x^{sr}-1=(x^r+1)(x^{r(s-1)}+x^{r(s-2)}+\ldots+x+1) \qquad x^{2r}-1=(x^r+1)(x^r-1)$$
$$y^k-1=(y-1)(y^{k-1}+y^{k-2}+\ldots+y+1) \qquad x^{3r}-1=(x^r-1)(x^{2r}+x^r+1)$$
$$x^{3r}+1=(x^r+1)(x^{2r}-x^r+1)$$

דואליות בפולינומים:

הגדרה: אם $f(x)$ פולינום מעל F_p, $\deg f(x)=n$, אזי **הדואלי** של $f(x)$ הוא $\bar{f}(x)=x^n f(\frac{1}{x})$
כלומר:
$$f(x)=a_nx^n+\ldots+a_1x+a_0,\ \bar{f}(x)=a_n+\ldots+a_1x^{n-1}+a_0x^n$$

טענה: $f(x)$ אי פריק $\Leftrightarrow$ $\bar{f}(x)$ אי-פריק.

טענה: $\bar{f}(x)\bar{g}(x)=\overline{f(x)g(x)}$ [הטענה אינה נכונה לחיבור].

טענה: אם $h(x)=g(x)f(x)$ אזי $\bar{h}(x)=\bar{g}(x)\bar{f}(x)$

כלל: אם a איבר בשדה סופי E עם p^n איברים ואם הסדר של a ב-$(E^*,*)$ הוא r, אזי הדרגה של הפולינום המינימלי של a, $g(x)$, שווה ל-d, כאשר d הוא המחלק המינימלי של n כך ש- $r \mid p^d-1$. $[F_p[a]:F_p]=d,\ |F_p(a)|=p^d$

טענה: מס' הפולינומים האי-פריקים מדרגה d וסדר r הוא $\frac{\phi(r)}{d}$.

תורת הקודים:

1. שליחת וקטור v פעמיים (v,v) כאשר בצד השני נקבל (v', v'') שאמורים להיות זהים - **קוד מגלה**.
2. v ← (v,v,v), בצד השני מקבלים (v', v'', v''') - אם שלושתם זהים זה בסדר. אם שניהם זהים והשלישי שונה בספרה אחת ← סביר להניח שהשניים האחרים בסדר וה-3 שגוי - **קוד מתקן**.

הגדרה: **קוד לינארי** (n, k) הוא קוד שבו כל מילות הקוד נמצאות במרחב וקטורי ממימד K בתוך F^n

הגדרה: אם v, w הן 2 מלים ב-F^n אז **המרחק** בין v ל-w, d(v,w), הוא מספר המרכיבים **השונים**.

הגדרה: **המרחק המינימלי** בקוד C הוא המינימום של המרחקים d(v,w) עבור $v,w\in C, v\neq w$.

משפט: בקוד לינארי המרחק המינימלי t הוא המרחק המינימלי בין מלים בקוד למלים שונות מ-0 לבין וקטור ה-0 (בגלל ש-(d(v,w) = d(v-w,0).

הגדרה: אם $v\in F^n$ אז המרחק בין v ל-(0,0,...,0) נקרא **המשקל** של v.

בניית קוד:

בניית **מטריצה יוצרת** G:
k איברי הבסיס כך ש-k העמודות **הראשונות נותנות** את מטריצת היחידה.
אם נתון וקטור מידע מאורך k: $m=(a_1,\ldots,a_k)$, $mG=(a_1,a_2,\ldots,a_k,a_{k+1},\ldots,a_n)$

משפט: נניח ש-C קוד לינארי שבו **המרחק המינימלי הוא t**, אז C יכול לגלות **t-1 שגיאות**, **ולתקן** $\left\lfloor\frac{t-1}{2}\right\rfloor$ **שגיאות**.

הגדרה: אם G מטריצה יוצרת

אז H מטריצת הביקורת

משפט: v' מילה בקוד $\Leftrightarrow$ v'H = 0.
מילה שגויה היא בעצם $w=v+ce_i$ ולכן $wH=(v+ce_i)H=0+c$(שורה i מתוך H).

משפט: אם במטריצת הבדיקה כל d-1 שורות בת"ל ויש d שורות ת"ל $\Leftarrow$ d(v) = d.

הגדרה: **קוד המינג:** בקוד המינג $k=n-c$, $n=2^c-1$, c=מס' ספרות הביקורת, המרחק המינימלי = 3.
למשל: אם c = 3 אזי הקוד הוא (7,4), c = 4 אזי הקוד הוא (15,11).
מטריצת הביקורת תכיל את כל הווקטורים מאורך c, פרט לוקטור ה-0.
למשל, כאשר c = 3:

<u>פענוח קוד לינארי:</u>

1. חישוב <u>הסינדרום</u>: s = w'H.
2. אם $s \neq 0$ מודיעים על טעות.
3. אם המרחק המינימלי גדול או שווה ל-3 $\Leftarrow$ ניתן לנסות לתקן (כי $\left\lfloor \frac{t-1}{2} \right\rfloor \geq 1$ כאשר t לפחות 3).
   א. אם t = 3,4 מחפשים את s כשורה במטריצה H ומשנים את הספרה בעמודה המתאימה ב-w'.
   ב. אם t = 5,6 אפשר לקבל 2 שורות. מנסים לקבל את הסינדרום s כסכום של שורה אחת i של H או 2 שורות i,j של H ומתקנים את i או את i,j.