

מעריך תירגול 9 - אלגברה מופשטת 2

1.0 חוגים אוקלידיים

הגדרה 0.1. יהי R תח"ש, פונקציה $d: R \rightarrow \mathbb{N} \cup \{-\infty\}$ המקיימת:

$$\bullet d(0) < d(x) \text{ לכל } x \in R, x \neq 0;$$

$$\bullet d(a) \leq d(ab);$$

$$\bullet \text{ לכל } b \neq 0 \text{ ולכל } a \text{ יש } q, r \text{ כך ש } a = qb + r \text{ ו } d(r) < d(b).$$

נקראת פונקציה אוקלידית. R נקרא חוג אוקלידי.

0.2 דוגמה $\mathbb{Z}, |\cdot|$

$$\bullet \mathbb{Z}[i], N$$

$$\bullet F[x], \deg(\cdot)$$

$$\bullet \mathbb{Z}[\sqrt{d}], |N| \text{ עבור } d = -1, \pm 2, \pm 3, -7, -11 \text{ למשל.}$$

(לא כל החוגים \mathcal{O}_d הם אוקלידים, וגם אלו שכן לא בהכרח אוקלידיים ביחס לנורמה).

טענה 0.3. אוקלידי \leftarrow ראשי \leftarrow תפ"י

איך ראשי? היוצר של אידיאל הוא האיבר מדרגה מינימלית.

דוגמא לחוג ראשי שאיננו אוקלידי: \mathcal{O}_{-19} .

טענה 0.4. $a \in R$ הפיך $\iff d(a) = d(1)$.

תרגיל 0.5. הוכיחו כי $F[[x]]$ הוא חוג אוקלידי ביחס ל

$$d\left(\sum_{n=0}^{\infty} a_n x^n\right) = \min\{i \mid a_i \neq 0\}$$
$$d(0) = -\infty$$

פתרון.

- ברור ש $d(0) < d(p(x))$ מההגדרה.
- קל לראות ש $d(p(x)) \leq d(p(x)q(x))$.
- יהיו $f(x), g(x)$ צריך למצוא $r(x), q(x)$ כך ש $f = qg + r$ עם $d(r) < d(g)$ אם $d(f) < d(g)$ אז פשוט ניקח $r = f$ ו $q = 0$ או $f = 0g + f$. אם $n = d(g) \leq d(f) = m$ אז נוכל לרשום

$$g(x) = a_n x^n + a_{n+1} x^{n+1} + \dots = x^n \underbrace{(a_n + a_{n+1} x + \dots)}_{g_0(x)}$$

נזכר ש g_0 הוא הפיך בחוג $F[[x]]$ (כי יש לו מקדם חופשי שונה מאפס).
 באותו אופן נוכל לרשום $f(x) = x^m f_0(x)$ אזי $f = (x^{m-n} f_0 g_0^{-1}) g + 0$ וסיימנו.

כאמור, האוקלידיות של חוג נותנת לנו כלי חישובי חזק: אלגוריתם אוקלידס. איתנו אפשר לחלק עם שארית ולמצוא gcd.

תרגיל 0.6. חשב את השארית בחילוק של $x = 15 + 11\sqrt{-2}$ ב $y = 4 - 3\sqrt{-2}$ ב $\mathbb{Z}[\sqrt{-2}]$ (שהוא כאמור אוקלידי ביחס לנורמה).

פתרון. כמו במרוכבים, נכפול בצמוד:

$$\frac{x}{y} = \frac{15 + 11\sqrt{-2}}{4 - 3\sqrt{-2}} \cdot \frac{4 + 3\sqrt{-2}}{4 + 3\sqrt{-2}} = \frac{-6 + 89\sqrt{-2}}{34} = \frac{-3}{17} + 2\frac{21}{34}\sqrt{-2}$$

אנחנו לוקחים את השלמים שהכי קרובים למקדמים:

$$\frac{x}{y} = \underbrace{0 + 3\sqrt{-2}}_q + \left(\frac{-3}{17} - \frac{13}{34}\sqrt{-2} \right)$$

השארית היא

$$r = x - yq = 15 + 11\sqrt{-2} - (4 - 3\sqrt{-2})(3\sqrt{-2}) = -3 - \sqrt{-2}$$

שימו לב שבאמת $N(r) = 9 + 2 = 11 < 34 = N(y)$.

אי פריקות פולינומים

מוטיבציה... להבהיר שהמנה זה מ"ו.

מינוח: על פולינום $f(x) \in R[x]$ אומרים שהוא **ב** $R[x]$ או **מעל** R . (ובאותו אופן פריק – לעומת פריק מעל-).

טענה 0.7. $f(x) \in F[x]$ מדרגה $n \geq 1$. f יש לכל היותר n שורשים ב F , ותמיד אפשר למצוא שדה $F \subseteq K$ שבו יש את כל השורשים.

(שימו לב שזה לא נכון מעל סתם חוגים, למשל ב $M_n(\mathbb{R})$ יש אינסוף פתרונות ל $x^2 = 0$).

טענה 0.8. עבור $f(x) \in F[x]$ ואיבר $c \in F$: $f(c) = 0$ אם ורק אם $(x - c) | f(x)$ מעל F . (זה נכון מעל כל חוג קומוטטיבי).

טענה 0.9. פולינום מדרגה 2,3 הוא אי-פריק \iff אין לו שורש.

זה כמובן לא נכון לדרגות גבוהות יותר: $(x^2 + 1)^2 \in \mathbb{R}[x]$ פריק אבל אין לו שורש ב \mathbb{R} .

דוגמה 0.10. $x^2 + x + 1$ א"פ מעל \mathbb{Z}_2 (כי הם לא שורשים שלו) אבל כן פריק מעל \mathbb{Z}_3 (כי 1 הוא שורש שלו) [למעשה $(x - 1)^2 = x^2 - 2x + 1 \equiv x^2 + x + 1$ מעל \mathbb{Z}_3].

1.1.0 פולינומים מעל תפ"י R

אנחנו מסמנים תמיד $F = q(R)$ שדה השברים. מה הקשר בין פירוק למעלה ופירוק למטה? האינטואיציה הראשונית היא לחשוב שלמעלה יותר דברים מתפרקים, כמו ש $x^2 + 1$ א"פ מעל \mathbb{R} אבל כן פריק במרוכבים. מסתבר שזה לא ממש ככה...

דוגמה 0.11. $2x + 2$ הוא פריק מעל \mathbb{Z} : $2x + 2 = 2(x + 1)$ וזה פירוק אמיתי. אבל מעל \mathbb{Q} הפירוק הנ"ל לא אמיתי (כי 2 הפיך) והפולינום אי פריק.

אבל ביננו לבין עצמנו, הפירוק הזה מעל \mathbb{Z} , הוא לא באמת "פיירי" ולכן אנחנו קוראים לפירוק של פולינום כשאחד הגורמים הוא איבר- פירוק לא אמיתי. פירוק אמיתי לש פולינומים הוא פירוק לגורמים מדרגות קטנות יותר. אז עכשיו נשאל: האם יכול להיות פולינום א"פ מעל F ושיש לו פירוק אמיתי מעל R ?

טענה 0.12. (אחד הטענות שקיבלו את השם הלמה של גאוס) פולינום $f(x) \in R[x]$ מדרגה $1 \leq n$ הוא אי-פריק מעל F אם ורק אם אין לו פירוק אמיתי מעל R .

מתי לפולינום אין פירוק לא אמיתי? למשל אם הוא מתוקן...

הגדרה 0.13. פולינום $f(x) = a_0 + a_1x + \dots + a_nx^n$ הוא פרימיטיבי אם התכולה שלו $c(f) = \gcd\{a_0, \dots, a_n\}$ (שמוגדרת עד כדי חברות) היא 1.

לפולינום פרימיטיבי אין פירוק לא אמיתי, ולכך אם הוא א"פ מעל F הוא גם א"פ מעל R .

עכשיו נשאר לנו לברר מתי פולינומים הם א"פ מעל F . בגדול, כמעט כל הפולינומים הם אי-פריקים אבל די קשה להוכיח שפולינום מסוים הוא אי-פריק. יש לנו בכל זאת 2-3 טריקים....

טענה 0.14. $p(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$. אם $\frac{\alpha}{\beta} \in F$ הוא שורש של $p(x)$ אז $\alpha|a_0$ ו $\beta|a_n$.

תרגיל 0.15. הוכח שלכל p ראשוני אי-זוגי, $\sqrt[n]{p}$ הוא לא רציונלי לכל $n > 1$.

פתרון. $\sqrt[n]{p}$ הוא שורש של הפולינום $x^n - p \in \mathbb{Z}[x]$. אם הוא היה רציונלי $\frac{\alpha}{\beta} = \sqrt[n]{p}$ אז לפי הטענה

$$\alpha|p \rightarrow \alpha = \pm 1, \pm p$$

$$\beta|1 \rightarrow \beta = \pm 1$$

אבל זה אומר ש $\sqrt[n]{p} = \pm p$ וזה כמובן לא נכון.

טענה 0.16. הקריטריון של אייזנשטיין:

יהי $p(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, $n \geq 1$. אם קיים אידיאל ראשוני $P \triangleleft R$ כך ש:

$$a_n \notin P \cdot$$

$$a_0, \dots, a_{n-1} \in P \cdot$$

$$a_0 \notin P^2 \cdot$$

אז $p(x)$ הוא אי פריק מעל F (ולכן אם הוא גם פרימיטיבי אז הוא א"פ גם מעל R).

ניסוח עבור החוג \mathbb{Z} :

אם יש מספר ראשוני p (יוצר של אידיאל ראשוני) כך ש:

$$p \nmid a_n \cdot$$

$$p|a_0, \dots, a_{n-1} \cdot$$

$$p^2 \nmid a_0 \cdot$$

אז הפולינום א"פ מעל \mathbb{Q} .

תרגיל 0.17. הוכח שהפולינומים הבאים הם א"פ מעל החוג המצויין:

$$1. \mathbb{Z}, x^5 - 4x^3 + 6$$

$$2. \mathbb{Z}, x^6 + 30x^5 - 15x^3 + 6x - 120$$

$$3. \frac{(x+2)^p - 2^p}{x} \text{ כאשר } p \text{ ראשוני אי-זוגי, } \mathbb{Z}$$

$$4. \mathbb{Z}[\sqrt{-2}], x^3 - 3$$

פתרון. 1. אייזנשטיין, 2 (להסביר לאט: 2 לא מחלק את המקדם העליון, מחלק את 4 ו 6, $2^2 = 4$, ו 6 לא מחלק את 6). לכן הוא א"פ מעל \mathbb{Q} , אבל הוא מתוקן ולכן הוא א"פ מעל \mathbb{Z} !

2. אייזנשטיין, 3.

$$3. \text{ נכתוב את הפולינום במפורש: } p(x) = \sum_{k=0}^{p-1} \binom{p}{k} 2^k x^{p-k-1}$$

$$\text{נשים לב ש } 2^k \mid \binom{p}{k} \text{ לכל } 1 \leq k \leq p-1$$

$$p^2 \nmid \binom{p}{p-1} 2^{p-1} = p 2^{p-1} \text{ ו } p \nmid \binom{p}{0}$$

ולכן הפולינום א"פ לפי אייזנשטיין עם p .

4. אם זה הוא מעל \mathbb{Z} , היינו משתמשים באייזנשטיין עם 3.

אבל 3 הוא לא ראשוני ב $\mathbb{Z}[\sqrt{-2}]$: $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$. אז נקח במקום את $p = 1 + \sqrt{-2}$ הוא אי-פריק כי הנורמה שלו $N(p) = 3$ היא אי-פריקה, ומכיוון שהחוג אוקלידי אז הוא גם ראשוני. והוא באמת מקיים את תנאי ק. אייזנשטיין.

טענה 0.18. יהיו $a, b \in R, 0 \neq a, b$

$$p(x) \in R[x] \text{ הוא א"פ אם } p(ax+b) \text{ א"פ.}$$

תרגיל 0.19. הוכיחו כי $p(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$ הוא א"פ מעל \mathbb{Z} .

פתרון. $p(x-1) = \dots = x^4 - 2x + 2$ הוא א"פ לפי אייזנשטיין עם 2.

תרגיל 0.20. הוכיחו כי $f(x, y) = y^2 + x^2y + 2y + x^4 + 5x^2 + 6$ הוא א"פ ב $\mathbb{Z}[x, y]$.

פתרון. נחשוב על החוג בתור $(\mathbb{Z}[x])[y]$ (פולינומים ב y עם מקדמים שהם פולינומים ב x),

$$\text{מנקודת המבט הזאת: } f(x, y) = y^2 + (x^2 + 2)y + (x^4 + 5x^2 + 6)$$

$$\text{נרצה להשתמש באייזנשטיין עם הגורם } p = x^2 + 2 \in \mathbb{Z}[x]$$

הוא באמת ראשוני כי הוא אי-פריק (למשל לפי אייזנשטיין עם 2), ו $\mathbb{Z}[x]$ הוא תפ"י.

והוא מקיים את דרישות ק. אייזנשטיין (בדקו!).

תרגיל 0.21. הוכיחו כי $x^n - y \in F[[x]][y]$ הוא אי-פריק/

פתרון. נרצה להשתמש באייזנשטיין עם $y \in F[[y]]$, לשם כך צריך להראות שהוא ראשוני. נראה קודם שהוא אי-פריק: אם בשלילה יש פירוק $y = \alpha(y)\beta(y) = (\sum_{n=0}^{\infty} a_n x^n) (\sum_{n=0}^{\infty} b_n x^n)$

$$\begin{cases} a_0 b_0 = 0 \\ a_0 b_1 + a_1 b_0 = 1 \end{cases} \quad \text{נשווה מקדמים}$$

מהמשוואה הראשונה נובע בה"כ ש $b_0 = 0$ ואז מהמשוואה השנייה $a_0 b_1 = 1$ מה שאומר ש $a_0 \neq 0$ ולכן $\alpha(y)$ הוא הפיך ב $F[[y]]$ — כלומר ש y הוא אי-פריק. ראינו ש $F[[y]]$ הוא אוקלידי (מספיק אפילו שהוא תפ"י) ולכן y גם ראשוני. כל מה שנשאר הוא לשים לב שהוא מקיים את ק.אייזנשטיין ולכן f הוא אי-פריק.