

פתרון מועד א' שנת תשעו

1. (א) הגדר הרחבה פשוטה של שדות.

פתרון: הרחבה K/F נקראת פשוטה אם קיים $a \in K$ כך ש $K = F(a)$.

(ב) יהי F שדה אין סופי. הוכח כי כל הרחבה ספרבילית סופית של F היא הרחבה פשוטה.

פתרון: תהי K/F ההרחבה המדוברת. נסמן ב E את סגור גלואה של K . E/F היא הרחבת גלואה סופית. לפי התאמת גלואה מספר שדות הביניים שווה למספר תתי החבורות של חבורת גלואה, כלומר זה מספר סופי (כי חבורת גלואה סופית). כל שדה ביניים של ההרחבה K/F הוא גם שדה ביניים של ההרחבה E/F ולכן ל K/F יש מספר סופי של שדות ביניים. מספיק להוכיח שאם $K = F(a, b)$ אז K פשוטה (ממשיכים באינדוקציה). לכל $t \in F$ נגדיר

$$c_t = a + tb$$

בגלל שיש אינסוף t יש אינסוף c_t . בגלל שיש רק מספר סופי של שדות ביניים, יש

$$t, t' \in F$$

כך ש $t \neq t'$ ו

$$F(c_t) = F(c_{t'})$$

ולכן

$$c_t - c_{t'} = (t - t')b \in F(c_t)$$

בגלל ש $t - t' \neq 0$ אפשר לצמצם בו ולקבל

$$b \in F(c_t)$$

אבל אז

$$a = c_t - tb \in F(c_t)$$

ולכן

$$F(c_t) = F(a, b)$$

כנדרש.

2. יהי $p(x) = x^{64} - x$ פולינום מעל F_2 . מצא כמה פולינומים אי פריקים מכל דרגה משתתפים בפירוק של $p(x)$ לגורמים אי פריקים.

פתרון: לפי משפט, מכפלת כל הפולינומים האי פריקים המתוקנים מעל F_p שדרגתם מחלקת את n הוא הפולינום

$$x^{p^n} - x$$

במקרה שלנו $p = 2$ בפרט כל פולינום אי פריק הוא מתוקן אז לא צריך להדגיש זאת. נסמן ב $q(n)$ את מספר הפולינום האי פריקים מסדר n . $q(1) = 2$ (שני הפולינומים $x, x + 1$ הם אי פריקים).

המכפלה של כל הפולינומים מדרגה שמחלקת את 2 היא

$$x^2 - x = x^4 - x$$

לפי השוואת דרגות

$$1q(1) + 2q(2) = 4$$

כלומר

$$2 + 2q(2) = 4$$

ולכן $q(2) = 1$ כלומר יש רק פולינום אחד אי פריק מדרגה 2. בדומה מכפלת הפולינומים מדרגה שמחלקת את 3 היא

$$x^8 - x$$

ולפי השוואת דרגות

$$1q(1) + 3q(3) = 8$$

כלומר

$$q(3) = 2$$

עכשיו נעשה את אותו חישוב עם 6:

$$1q(1) + 2q(2) + 3q(3) + 6q(6) = 2^6$$

ולכן

$$2 + 2 + 6 + 6q(6) = 64$$

$$q(6) = 9$$

ובזה סיימנו.

אני רוצה להוסיף כאן הוכחה לטענה שלמעלה. כלומר: אם $f(x)$ פולינום אי פריק מעל F_p אז $f(x) \mid x^{p^n} - x$ אם ורק אם $\deg f(x) \mid n$.

טענת עזר (שלא אוכיח): $x^m - 1 \mid x^n - 1$ אם ורק אם $m \mid n$. בדומה עבור מספרים טבעיים, $k^m - 1 \mid k^n - 1$ אם ורק אם $k \mid n$.

טענת עזר 2: $x^{p^m} - x \mid x^{p^n} - x$ אם ורק אם $m \mid n$. הוכחה: $x^{p^m} - x \mid x^{p^{m-1}} - 1$ אם ורק אם $x^{p^m} - x \mid x^{p^{n-1}} - 1$ אם ורק אם $x^{p^m} - x \mid x^{p^n} - x$ אם ורק אם $m \mid n$.

עכשיו ההוכחה: נניח ש $f(x)$ אי פריק מעל F_p מדרגה d . ויהי α שורש שלו. אז שדה $K = F_p[x]/\langle f(x) \rangle = F_p(\alpha)$ הוא שדה ממימד d כלומר בגודל p^d . כלומר זה שדה הפיצול של $x^{p^d} - x$. כל השורשים של $f(x)$ נמצאים ב K (זו הרי הרחבת גלואה - השדות סופיים) כלומר כל השורשים של $f(x)$ הם גם שורשים של $x^{p^d} - x$. צד ראשון: נניח ש $d \mid n$ אז היות ש $f(x)$ ספרבילי (פולינום אי פריק מעל שדה סופי תמיד ספרבילי) מתקיים ש

$$f(x) \mid x^{p^d} - x \mid x^{p^n} - x$$

מצד שני, נניח ש $f(x) \mid x^{p^n} - x$. כלומר כל השורשים של f ובפרט α מקיים ש $\alpha^{p^n} = \alpha$. אבל $K = F_p(\alpha)$ בגלל שגם α מתקבעים תחת האוטומורפיזם $x \rightarrow x^{p^n}$ ולכן

$$x^{p^d} - x \mid x^{p^n} - x$$

וזה מכריח $d \mid n$.

3. יהי $p(x) = x^4 - 7$ פולינום מעל \mathbb{Q} .

(א) מצא את שדה הפיצול E של $p(x)$ וחשב את $[E : \mathbb{Q}]$.
פתרון: השורשים של הפולינום הם $\sqrt[4]{7}, \sqrt[4]{7}i, -\sqrt[4]{7}, -\sqrt[4]{7}i$ ולכן

$$E = \mathbb{Q}(\sqrt[4]{7}, \sqrt[4]{7}i, -\sqrt[4]{7}, -\sqrt[4]{7}i)$$

כמובן שזה שווה ל

$$E = \mathbb{Q}(\sqrt[4]{7}, i)$$

כמובן ש

$$[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 4$$

(כי $x^4 - 7$ אי פריק לפי אייזנשטיין). ובנוסף

$$i \notin \mathbb{Q}(\sqrt[4]{7})$$

כי זה שדה של מספרים ממשיים. ולכן הפולינום המינימלי של i מעל השדה הנ"ל הוא $x^2 + 1$ ולכן

$$[E : \mathbb{Q}(\sqrt[4]{7})] = 2$$

לפי הכפלות

$$[E : \mathbb{Q}] = 8$$

(ב) חשב את $\text{Gal}(E/\mathbb{Q})$ על ידי מציאת יוצרים ויחסים (יש לפרט את פעולות היוצרים על שורשי הפולינום). מהי החבורה שקיבלתם?

פתרון: ראשית נשים לב שזאת הרחבת גלואה (שדה פיצול של פולינום ספרבילי). ולכן גודל חבורת גלואה הוא 8. כעת, נשים לב שהצמדה מרוכבת $\tau(a+bi) = a-bi$ היא אוטומורפיזם לא טריוויאלי של השדה מסדר 2. בנוסף, נשים לב ש $x^4 - 7$ הוא הפולינום המינימלי של $\sqrt[4]{7}$ מעל $\mathbb{Q}(i)$ (המימד של ההרחבה הוא 4 משיקולי כפלויות ולכן הפולינום צריך להיות אי פריק). היות שחבורת גלואה $\text{Gal}(E/\mathbb{Q}(i))$ פועלת באופן טרנזיטיבי על השורשים אנחנו יודעים שיש אוטומורפיזם σ המקיים

$$\sigma(\sqrt[4]{7}) = \sqrt[4]{7}i, \quad \sigma(i) = i$$

נשים לב שהסדר של σ הוא 4. נשים לב ש $\tau \notin \langle \sigma \rangle$ (משום ש σ מקבע את i ולכן

$$\langle \tau, \sigma \rangle$$

היא חבורה מסדר גדול מ-4 אבל היא תת חבורה של חבורת גלואה G שהיא מסדר 8 ולכן

$$\langle \tau, \sigma \rangle = G$$

עכשיו צריך להבין מה החבורה. זה ניחוש סביר שהיא תהיה D_4 . נוכיח זאת. נמספר את שורשי הפולינום $x^4 - 7$ לפי הסדר שהם כתובים למעלה. לפי זה,

$$\sigma = (1234), \quad \tau = (24)$$

ניתן לראות שתמורות אלו פורשות את D_4 (כי הן סימטריות של ריבוע - סיבוב ושיקוף). אפשר גם לבדוק לפי יוצרים ויחסים (כמו שמבקשים בשאלה)

$$\sigma^4 = 1, \quad \tau^2 = 1$$

ובנוסף

$$\tau\sigma = (12)(34) = \sigma^3\tau$$

(ג) מצאו 5 שדות ביניים. יש לתת יוצרים לכל שדה ומימד מעל \mathbb{Q} . **פתרון:** קל למצוא שדות ביניים גם בלי שימוש מפורש בהתאמת גלואה. יש לנו את

$$\mathbb{Q}(i), \mathbb{Q}(\sqrt{7})$$

שהם בוודאי שונים ושניהם ממימד 2 מעל \mathbb{Q} . יש לנו את

$$\mathbb{Q}(i, \sqrt{7}), \mathbb{Q}(\sqrt[4]{7})$$

שהם גם בוודאי שונים וממימד 4 מעל \mathbb{Q} . ובנוסף יש לנו את $\mathbb{Q}(\sqrt{7}i)$ שהוא ממימד 2 מעל \mathbb{Q} . די ברור שהוא שונה מ-2 אלה למעלה (כי אם שדה כולל גם את $\sqrt{7}i$ וגם את i הוא כולל את $\mathbb{Q}(i, \sqrt{7})$ ואם שדה כולל את $\sqrt{7}i$ ואת $\sqrt[4]{7}$ קל לראות שהוא כל E).

4. תהי K הרחבת שדות ממימד p מעל השדה F_p ותהי $G = \langle \sigma \rangle$ חבורת הגלואה של ההרחבה.

(א) חשבו על σ כעל אופרטור לינארי הפועל על K וחשבו את הפולינום האופייני שלו.

(ב) הוכיחו כי $\sigma - 1$ נילפוטנטי מסדר p ולכן לפי אלגברה לינארית קיים בסיס B של K כך שהמטריצה המייצגת $[\sigma - 1]_B$ היא בלוק ז'ורדן מסדר p .

(ג) השתמשו בסעיף ב על מנת למצוא את $[\sigma]_B$.

(ד) השתמשו בסעיף ג על מנת להוכיח שקיים $x \in K$ כך ש $\sigma(x) = x + 1$.

פתרון:

i. כזכור חבורת גלואה של שדה סופי מעל F_p היא חבורה ציקלית $G = \langle \sigma \rangle$ הנוצרת על ידי אוטומורפיזם פרובניוס

$$\sigma(x) = x^p$$

הסדר של G הוא p משום ש

$$|G| = [K : F_p] = p$$

ולכן $\sigma^p = \text{id}$ כלומר $\sigma^p - \text{id} = 0$ ולכן $(\sigma - \text{id})^p = 0$ (כי במאפיין p מתקיים $(x + y)^p = x^p + y^p$). כלומר הפולינום $(x - 1)^p$ מאפס את σ . מזה לומדים שהפולינום המינימלי הוא מהצורה $(x - 1)^m$ כלשהוא ולכן הפולינום האופייני הוא $(x - 1)^p$ (כל גורם של הפולינום המינימלי צריך להיות בפולינום האופייני).

ii. עכשיו, ברור ש $\sigma - \text{id}$ הוא נילפוטנטי (כי מתקיים $(\sigma - \text{id})^p = 0$) מה שצריך להוכיח זה שהסדר הוא p כלומר $m = p$. מספיק להוכיח שהריבוי הגאומטרי (של הע"ע היחיד 0) הוא 1 (כי זה מספר הבלוקים בצורת ז'ורדן). המרחב העצמי של 0 הם אותם $x \in K$ המקיימים $(\sigma - \text{id})(x) = 0$ כלומר $\sigma(x) = x$ כלומר $x^p = x$. לפולינום הזה יש לכל היותר p פתרונות, שהם בדיוק השדה F_p והוא אכן ממימד 1 מעל F_p .

iii. ברור ש

$$[\sigma]_B = \begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}$$

i. נסמן את איברי הבסיס $B = \{b_1, b_2, \dots, b_p\}$ שימו לב ש

$$\sigma(b_1) = b_1$$

ולכן $b_1 \in F_p$ בלי הגבלת כלליות אפשר להניח $b_1 = 1$ (אחרת אפשר לכפול אותו בסקלר) ואז נקבל ש

$$\sigma(b_2) = b_2 + b_1 = b_2 + 1$$

כנדרש.