פתרון תרגיל בית 2 בשדות ותורת גלואה
88-311 סמסטר א' תשפ"ב

שאלה 1. הוכיחו כי לפולינום $f(x)=(x^2-2)(x^2-3)(x^2-6)$ אין שורשים ב-$\mathbb{Q}$, אבל יש לו שורשים ב-$\mathbb{F}_p$ לכל p ראשוני.

פתרון. קל לראות שלפולינום הזה אין שורשים ב-$\mathbb{Q}$, כי השורשים הממשיים שלו הם המספרים $\pm\sqrt{2},\pm\sqrt{3},\pm\sqrt{6}$ שאינם רציונליים. מודולו p, אם $p=2$ אז $0,1$ שורשים שלו. אחרת, ל-f יש שורש אם ורק אם לפחות אחד מבין $\sqrt{2},\sqrt{3},\sqrt{6}\in\mathbb{F}_p$ (כלומר לפחות אחד מהמספרים 2, 3 או 6 הוא ריבוע מודולו p). מאותו נימוק שראינו בתרגול, אם 2 ו-3 אינם ריבועים מודולו p, שניהם שייכים למחלקה הלא טריוויאלית של $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2\cong\mathbb{Z}/2\mathbb{Z}$, ולכן מכפלתם, 6, שייכת למחלקה הטריוויאלית, כלומר ריבוע מודולו 6.

שאלה 2. יהיו $f(x)=x^2-3x+3, g(x)=x^3+2x+5\in\mathbb{Q}[x]$.
תזכורת: אלגוריתם אוקלידס המורחב עובד בתחומים אוקלידיים כמו $F[x]$.

א. מצאו את $\gcd(f(x),g(x))$.

ב. מצאו את ההופכי של $g(x)$ בשדה $\mathbb{Q}[x]/\langle f(x)\rangle$.

פתרון.

א. נעזר בתזכורת, ונשתמש באלגוריתם אוקלידס עם הערות לחישוב בסוגריים מרובעים:

$$\begin{aligned}
\gcd(g(x),f(x)) &= \left[x^3+2x+5=(x+3)(x^2-3x+3)+8x-4\right]\\
\gcd(f(x),8x-4) &= \left[x^2-3x+3=(\frac{1}{8}x-\frac{5}{16})(8x-4)+\frac{7}{4}\right]\\
\gcd(8x-4,\frac{7}{4}) &= \left[8x-4=(\frac{32}{7}x-\frac{16}{7})\cdot\frac{7}{4}+0\right]\\
\gcd(\frac{7}{4},0) &= 1
\end{aligned}$$

כלומר הפולינומים זרים (שימו לב ש-1 וגם $\frac{7}{4}$ הפיכים ב-$\mathbb{Q}[x]$).

ב. צריך להשתמש באלגוריתם אוקלידס המורחב ולבחור את מקדם בזו המתאים. נחשב את המקדמים

$$\begin{aligned}
8x-4 &= 1\cdot(x^3+2x+5)-(x+3)(x^2-3x+3)\\
\frac{7}{4} &= 1\cdot(x^2-3x+3)-(\frac{1}{8}x-\frac{5}{16})(8x-4)\\
&= 1\cdot(x^2-3x+3)-(\frac{1}{8}x-\frac{5}{16})(1\cdot(x^3+2x+5)-(x+3)(x^2-3x+3))\\
&= (\frac{1}{8}x^2+\frac{1}{16}x+\frac{1}{16})(x^2-3x+3)+(-\frac{1}{8}x+\frac{5}{16})(x^3+2x+5)
\end{aligned}$$

נכפיל ב-$\frac{4}{7}$ את המשוואה האחרונה, ונקבל

$$\gcd(f(x),g(x))=1=(\frac{1}{14}x^2+\frac{1}{28}x+\frac{1}{28})f(x)+(-\frac{1}{14}x+\frac{5}{28})g(x)$$

ולכן האיבר ההופכי הוא $\langle f(x)\rangle+(-\frac{1}{14}x+\frac{5}{28})$.

שאלה 3. תהי K/F הרחבת שדות. נתבונן בחוג הפולינומים $K[x]$ ובשדה הפונקציות הרציונליות $F(x)$, ונחשוב על שניהם כתת־קבוצות של השדה $K(x)$ באופן הברור. הוכיחו $F(x)\cap K[x]=F[x]$.

פתרון. הוכחת ההכלה ($\supseteq$) קלה כי כל פולינום מעל F הוא פולינום מעל K וגם פונקציה רציונלית מעל F.

להכלה ($\subseteq$) נשים לב שלפונקציה רציונלית מעל F (ששייכת ל-$K(x)$) שהיא גם פולינום מעל K יש מכנה 1 ומונה שהוא פולינום מעל F, כלומר פולינום מעל F שנמצא ב-$K(x)$.

שאלה 4. תהי K/F הרחבת שדות, ויהי $a\in K$. הוכיחו או הפריכו את הטענות הבאות:

א. אם a איבר אלגברי מעל K אז הוא אלגברי מעל F.

ב. אם a איבר אלגברי מעל F אז הוא אלגברי מעל K.

ג. אם a איבר אלגברי מעל F אז גם $\alpha\cdot a$ הוא אלגברי לכל $\alpha\in F$.

פתרון.

א. הפרכה: π הוא אלגברי מעל $K=\mathbb{R}$ כי הוא מאפס את הפולינום $x-\pi$, אבל הוא לא אלגברי מעל $\mathbb{Q}$. דוגמה אחרת, שאולי היא יותר פשוטה, זה ש-x אלגברי מעל $\mathbb{C}(x)$, אבל לא מעל $\mathbb{C}$.

ב. הוכחה: a אלגברי מעל F ולכן יש פולינום $p(x)\in F[x]$ כך ש-$p(a)=0$. אבל $F\subseteq K$ ולכן $p(x)\in K[x]$. כלומר שיש פולינום מעל K שמתאפס ב-a ולכן a אלגברי מעל K.

ג. הוכחה: a אלגברי ולכן יש $p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$ כך ש-$p(a)=0$. אז

$$0=p(a)=\frac{1}{\alpha^n}(\alpha a)^n+a_{n-1}\frac{1}{\alpha^{n-1}}(\alpha a)^{n-1}+\cdots+a_1\frac{1}{\alpha}(\alpha a)+a_0$$

שהרי $\alpha^{-i}\cdot(\alpha a)^i=a^i$. נשים לב ש-$a_i\frac{1}{\alpha^j}\in F$ לכל i,j. לכן

$$q(x)=\frac{1}{\alpha^n}x^n+\frac{a_{n-1}}{\alpha^{n-1}}x^{n-1}+\cdots+\frac{a_1}{\alpha}x+a_0$$

הוא פולינום מעל F שמתאפס ב-αa.

שאלה 5. תהי K/F הרחבה סופית (כלומר $[K:F]<\infty$). הוכיחו כי כל איבר של K הוא אלגברי מעל F. רמז: חשבו על הקבוצה $\{1,a,a^2,a^3,\dots\}$.
רשות: להרחבה כמו בשאלה קוראים הרחבה אלגברית. האם כל הרחבה אלגברית היא סופית?

פתרון. יהי $a\in K$. מכיוון שדרגת ההרחבה סופית, הקבוצה $\{1,a,a^2,\dots\}$ חייבת להיות תלויה לינארית מעל F. כלומר יש צירוף לינארי לא טריוויאלי של החזקות שמתאפס:

$$b_na^n+b_{n-1}a^{n-1}+\cdots+b_0=0$$

ולכן $b_nx^n+\cdots+b_0\in F[x]$ הוא פולינום שמתאפס ב-a. כלומר a אלגברי מעל F, כדרוש.

שאלה 6. הוכיחו כי $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)=\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$.

פתרון. ברור כי $\sqrt{2}+\sqrt{3}\in\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ ולכן $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)\supseteq\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$. מצד שני

$$\left(\sqrt{2}+\sqrt{3}\right)^2=2+2\sqrt{2}\sqrt{3}+3=2\sqrt{6}+5$$

ולכן $\sqrt{6}\in\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$. בנוסף $\sqrt{6}\left(\sqrt{2}+\sqrt{3}\right)=2\sqrt{3}+3\sqrt{2}$ ולכן

$$2\sqrt{3}+3\sqrt{2}-2\left(\sqrt{2}+\sqrt{3}\right)=\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$$

ובוודאי

$$\sqrt{3}=\sqrt{2}+\sqrt{3}-\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$$

ולכן $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)\subseteq\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$, כנדרש. הזכרו שאם α אלגברי מעל F, אז $F[\alpha]=F(\alpha)$, ולכן הסתפקנו "רק" בהוכחת $\mathbb{Q}\left[\sqrt{2},\sqrt{3}\right]=\mathbb{Q}\left[\sqrt{2}+\sqrt{3}\right]$.

שאלה 7. יהי F שדה, ותהי $G\leq F^*$ תת־חבורה סופית של החבורה הכפלית של השדה. הוכיחו כי G ציקלית. הדרכה: העזרו בתורת המבנה של חבורות אבליות סופיות ובחישוב $\exp(G)$.

פתרון. לפי משפט המבנה של חבורות אבליות סופיות, ניתן להציג את G כמכפלה

$$G\cong\left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right)\times\left(\mathbb{Z}/p_2^{k_2}\mathbb{Z}\right)\times\cdots\times\left(\mathbb{Z}/p_t^{k_t}\mathbb{Z}\right)$$

כאשר $p_1,\ldots,p_t$ ראשוניים כלשהם (אולי שווים) ו־$k_1,\ldots,k_t\in\mathbb{N}$. נסמן

$$m=\operatorname{lcm}(p_1^{k_1},p_2^{k_2},\ldots,p_t^{k_t})$$

וכידוע לנו מתורת החבורות $\exp(G)=m$ ולכן $m\leq|G|$. כלומר $x^m=e_G$ לכל $x\in G$. אבל לפולינום x^m-1 ישנם לכל היותר m פתרונות בשדה F. כלומר $|G|\leq m$, וקיבלנו $|G|=m$. לכן בהכרח $p_i\neq p_j$ לכל $i\neq j$, שכן אחרת

$$m=\operatorname{lcm}(p_1^{k_1},p_2^{k_2},\ldots,p_t^{k_t})<p_1^{k_1}p_2^{k_2}\ldots p_t^{k_t}=|G|$$

וקיבלנו ש־G היא מכפלה ישרה של חבורות ציקליות מסדרים זרים בזוגות. לפי משפט השאריות הסיני נסיק שהיא ציקלית מסדר $p_1^{k_1}p_2^{k_2}\ldots p_t^{k_t}$.

בהצלחה!