אלגברה מופשטת 3 – תרגיל 7

שאלה 1

יהי K שדה הפיצול של x^5-10 מעל $\mathbb{Q}$. מצאו שני איברים ב-$Gal(K/\mathbb{Q})$ היוצרים את $Gal(K/\mathbb{Q})$ (**<u>אין צורך למצוא את כל החבורה!</u>**). עליכם לייצג האיברים שמצאתם בשתי דרכים: ע"י הפעולה שלהם על היוצרים של ההרחבה וע"י הפעולה שלהם על השורשים של x^5-10. בנוסף, <u>הראו כי $Gal(K/\mathbb{Q})$ לא אבלית</u>.

הדרכה: אם G חבורה ו-$a_1,\dots,a_r$ איברים ב-G כך ש-$|G|=\operatorname{lcm}(o(a_1),\dots,o(a_r))$ אז $a_1,\dots,a_r$ יוצרים את G. [תזכורת: $o(a)=\min\{n\in\mathbb{N}\mid a^n=e\}=|\langle a\rangle|$.] נסו להפעיל רעיון זה עבור $G=Gal(K/\mathbb{Q})$.

פיתרון

הפולינום x^5-10 אי פריק (מדוע?). השורשים שלו הם $\sqrt[5]{10},\rho_5\sqrt[5]{10},\rho_5^2\sqrt[5]{10},\rho_5^3\sqrt[5]{10},\rho_5^4\sqrt[5]{10}$. לכן $K=\mathbb{Q}[\sqrt[5]{10},\rho_5\sqrt[5]{10},\rho_5^2\sqrt[5]{10},\rho_5^3\sqrt[5]{10},\rho_5^4\sqrt[5]{10}]=\mathbb{Q}[\sqrt[5]{10},\rho_5]$. יהי $n=[K:\mathbb{Q}]$, אזי n מתחלק ב- $[\mathbb{Q}[\sqrt[5]{10}]:\mathbb{Q}]=5$ וב-$[\mathbb{Q}[\rho_5]:\mathbb{Q}]=4$ (הפולינום המינימלי של ρ_5 מעל $\mathbb{Q}$ הוא מדרגה 4). מצד שני, $n=\left[\mathbb{Q}[\sqrt[5]{10},\rho_5]:\mathbb{Q}[\rho_5]\right]\cdot[\mathbb{Q}[\rho_5]:\mathbb{Q}]\le\left[\mathbb{Q}[\sqrt[5]{10}]:\mathbb{Q}\right]\cdot 4=5\cdot 4=20$. לכן בהכרח $n=20$. זה אומר שב-$G\coloneqq Gal(K/\mathbb{Q})$ יש 20 איברים.

כל איבר ב-G נקבע לפי הפעולה שלו על $\sqrt[5]{10}$ ו-ρ_5. $\sqrt[5]{10}$ יכול להישלח ע"י איבר של G רק אל הקבוצה $A=\{\sqrt[5]{10},\rho_5\sqrt[5]{10},\rho_5^2\sqrt[5]{10},\rho_5^3\sqrt[5]{10},\rho_5^4\sqrt[5]{10}\}$ ו-ρ_5 יכול להישלח ע"י איבר של G רק אל קבוצת שורשי היחידה הפרימיטיביים מסדר 5, כלומר אל $B=\{\rho_5,\rho_5^2,\rho_5^3,\rho_5^4\}$. היות וב-$G$ 20 איברים שונים, בהכרח לכל $a\in A,b\in B$ קיים $\sigma\in G$ המקיים $\sigma\sqrt[5]{10}=a,\ \sigma\rho_5=b$.

תהיינה $\sigma,\tau\in G$ ההעתקות המקיימות:

- $\sigma\sqrt[5]{10}=\rho_5\sqrt[5]{10},\ \sigma\rho_5=\rho_5$
- $\tau\sqrt[5]{10}=\sqrt[5]{10},\ \tau\rho_5=\rho_5^2$

נמספר את השורשים $\sqrt[5]{10},\rho_5\sqrt[5]{10},\rho_5^2\sqrt[5]{10},\rho_5^3\sqrt[5]{10},\rho_5^4\sqrt[5]{10}$ ב-1,2,3,4,5 בהתאמה. אזי:

- התמורה המתאימה ל-σ היא $(1,2,3,4,5)$.
- התמורה המתאימה ל-τ היא $(2,3,5,4)$. [הסבר: $\tau(\rho_5^i\sqrt[5]{10})=\tau(\rho_5)^i\tau(\sqrt[5]{10})=(\rho_5^2)^i\sqrt[5]{10}=\rho_5^{2i}\sqrt[5]{10}$.]

לכן, $ord(\tau)=4$, $ord(\sigma)=5$. גודל החבורה $<\tau,\sigma>$ מתחלק ב-$ord(\sigma),ord(\tau)$ ולכן חייב להתחלק ב-5 וב-4, כלומר להתחלק ב-20. היות ו-$|G|=20$ זה אומר ש-$G=<\tau,\sigma>$.

הערה: אפשר לבדוק ישירות ע"י הפעולה של σ,τ על היוצרים של K ש-$ord(\sigma)=5,ord(\tau)=4$.

החבורה G לא אבלית כי $(1,2,4,3)=(1,2,3,4,5)(2,3,5,4)$ אבל $(2,3,5,4)(1,2,3,4,5)=(1,3,2,5)$. (כלומר, $\sigma\tau\neq\tau\sigma$).

שאלה 2

יהי $K=\mathbb{Q}[\sqrt[7]{5}]$. הראו כי $Gal(K/\mathbb{Q})=\{id_K\}$. מדוע גודל החבורה לא שווה ל-$[K:\mathbb{Q}]$?

פיתרון

קודם נראה שהשורש היחיד של x^7-5 שנמצא ב-K הוא $\sqrt[7]{5}$. באמת, שורשי הפולינום ב-$\mathbb{C}$ (שמכיל את K) הם $\sqrt[7]{5},\rho_7\sqrt[7]{5},\dots,\rho_7^6\sqrt[7]{5}$ (באשר $\rho_7=\exp\left(\frac{2\pi i}{7}\right)$). השורש היחיד ששייך ל-$\mathbb{R}$ הוא $\sqrt[7]{5}$ ולכן הוא גם היחיד ששייך ל-K.

דרך אחרת להראות זאת ללא שימוש במרוכבים: נניח ש-$\alpha\in K$ מקיים $\alpha^7=5$, אזי $\left(\frac{\alpha}{\sqrt[7]{5}}\right)^7=\frac{5}{5}=1$, כלומר $\beta:=\frac{\alpha}{\sqrt[7]{5}}$ הוא שורש של $x^7-1=(x-1)(x^6+\cdots+x+1)$. אם $\beta\neq 1$, אז הוא שורש של $x^6+\cdots+x+1$. זה פולינום אי פריק ולכן מתקיים $[\mathbb{Q}[\beta]:\mathbb{Q}]=\deg(x^6+\cdots+x+1)=6$, אבל $[\mathbb{Q}[\beta]:\mathbb{Q}]$ חייב להתחלק ב-$[K:\mathbb{Q}]=7$ ולכן קיבלנו סתירה. לכן בהכרח $\beta=1$ ו-$\alpha=\sqrt[7]{5}$.

ברור ש-$id_K\in Gal(K/\mathbb{Q})$. מצד שני, אם $\sigma\in Gal(K/\mathbb{Q})$ אז $\sigma(\sqrt[7]{5})$ הוא שורש של x^7-5. לפי מה שהראינו מקודם, נובע ש-$\sigma(\sqrt[7]{5})=\sqrt[7]{5}$. היות ו-$K=\mathbb{Q}[\sqrt[7]{5}]$, אז $\sigma=id_K$.

גודל החבורה אינו שווה ל-$[K:\mathbb{Q}]=7$ כי K אינו שדה פיצול (לא של x^7-5 ובהכרח גם לא של אף פולינום אחר).

שאלה 3

יהי p ראשוני ו-$F=\mathbb{Z}_p(t)$ (שדה הפונקציות הרציונליות מעל $\mathbb{Z}_p$ במשתנה t, כלומר שדה השברים של $\mathbb{Z}_p[t]$). נגדיר $f(x)\in F[x]$ ע"י $f(x)=x^p-t$.

1. הראו כי f אי פריק.
2. יהי $E=F[x]/\langle f(x)\rangle$. הראו כי E שדה פיצול של f. [רמז: לכל $a(x),b(x)\in F[x]$ מתקיים $\left(a(x)+b(x)\right)^p=a(x)^p+b(x)^p$.]
3. הראו כי $Gal(E/F)=\{id_E\}$. מדוע גודל החבורה לא שווה ל-$[E:F]$?

פיתרון

הוכחת 1: x^p-t הוא פולינום אייזנשטיין ביחס לראשוני t ולכן אי פריק. (השתמשנו כאן בעובדה ש-$\mathbb{Z}_p[t]$ הוא תחום פריקות יחידה וכן בעובדה שכל פולינום ממעלה 1 הוא ראשוני [אין צורך להוכיח זאת].) **משל.**

הוכחת 2: נסמן $a=x+\langle f(x)\rangle\in E$. אזי a שורש של f ולכן $a^p=t$. היות והמאפיין של E הוא $p>0$ מתקיים: $(x-a)^p=x^p-a^p=x^p-t=f(x)$ (ולכן f מתפצל מעל E). זה אומר שהשורש היחיד של f הוא a ולכן, שדה הפיצול של f הוא $E=F[a]$ (השוויון נובע מהגדרת E ומטענה שאמרנו בתרגול ממזמן). **משל.**

הערה: קל גם להוכיח ישירות שאין ל-E תת שדה מעליו f מתפצל.

הוכחת 3: ברור ש-$id_E\in Gal(E/F)$. מצד שני, יהי $\sigma\in Gal(E/F)$, אזי σa הוא שורש של $\sigma f=f$. לפי סעיף 2, זה אומר ש-$\sigma a=a$ (כי a הוא השורש היחיד של f). היות ו-$E=F[a]$ (סעיף 2), נובע ש-$\sigma(u)=u$ לכל $u\in E$, כלומר $\sigma=id_E$. **משל.**

גודל החבורה לא שווה ל-p למרות ש-$[E:F] = p$ שדה פיצול של f כי הפולינום f אינו ספרבילי, כפי שהוכח בסעיף 2.