

אלגברה מופשטת 3 – תרגול 7

משפט: $Gal(\mathbb{Q}(\rho_n)/\mathbb{Q}) = U(\mathbb{Z}_n)$.

מסקנה: $Gal(\mathbb{Q}(\rho_p)/\mathbb{Q}) = U(\mathbb{Z}_p) = \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$. השייון האחרון מימין הוא בגלל ש \mathbb{Z}_p^* היא תת-חבורה סופית כפלית של שדה ולכן ציקלית.

תרגיל: חשבו את החבורה $Gal(E/\mathbb{Q})$ (עד כדי איזומורפיזם) כאשר E/\mathbb{Q} הוא שדה הפיצול של $f(x) = x^5 - 7 \in \mathbb{Q}[x]$.

פתרון: כבר ידוע לנו שמתקיים $E = \mathbb{Q}(\sqrt[5]{7}, \rho_5)$. נסמן $G = Gal(E/\mathbb{Q})$ מדובר בתת-חבורה מסדר 20 של S_5 הפועלת טרנזיטיבית על $\{1, \dots, 5\}$. בנוסף יש לנו בהכרח איבר מסדר 5, כי $5 = [\mathbb{Q}(\sqrt[5]{7}) : \mathbb{Q}] | [E : \mathbb{Q}] = |Gal(E/\mathbb{Q})|$ ולכן בהכרח קיים בחבורה מחזור מסדר 5. בנוסף יש לנו איבר מסדר 4 בחבורה G , כיוון ש $Gal(E/\mathbb{Q}(\sqrt[5]{7})) \cong \mathbb{Z}_4$, נסביר מדוע:

$Gal(\mathbb{Q}(\rho_5)/\mathbb{Q}) \cong \mathbb{Z}_4$ לפי המסקנה מהמשפט. בנוסף קיים שיכון $Gal(E/\mathbb{Q}(\sqrt[5]{7})) \rightarrow Gal(\mathbb{Q}(\rho_5)/\mathbb{Q}) \cong \mathbb{Z}_4$, כי ניתן לצמצם כל $\sigma \in Gal(E/\mathbb{Q}(\sqrt[5]{7}))$ לשדה $\mathbb{Q}(\rho_5)$, כיוון שמדובר בהרחבת גלואה של \mathbb{Q} . אבל הצמצום הוא חח"ע כי אם הוא קובע את ρ_5 הוא חייב להיות הזהות כי הוא קובע גם את $\sqrt[5]{7}$. אבל Φ_5 נשאר אי-פריק מעל $\mathbb{Q}(\sqrt[5]{7})$ ולכן ההרחבה $E/\mathbb{Q}(\sqrt[5]{7})$ היא מדרגה 4, ולכן החבורות שוות.

למעשה קל להציג את האוטומורפיזמים האלה במפורש. $\sqrt[5]{7} \mapsto \sqrt[5]{7}, \rho_5 \mapsto \rho_5^2$, זהו אוטומורפיזם מסדר 4 (בדקו זאת). בנוסף יש לנו איבר מסדר 5 והוא $\rho_5 \sqrt[5]{7} \mapsto \rho_5 \sqrt[5]{7}, \rho_5 \mapsto \rho_5$. כעת מתקיים $\langle \sigma, \tau \rangle = G$ (כי סדרי האיברים זרים). בנוסף $\sqrt[5]{7} \mapsto \rho_5^2 \sqrt[5]{7}, \rho_5 \mapsto \rho_5$, כלומר מתקיים $\sigma^2 = \tau \sigma \tau^{-1}$. לכן מתקיים (הצגה של חבורה ע"י יוצרים ויחסים) $\langle \sigma, \tau \mid \sigma^5 = \tau^4 = 1, \tau \sigma \tau^{-1} = \sigma^2 \rangle$.

תרגיל: יהי $f(x) \in \mathbb{Q}[x]$ פולינום אי-פריק מדרגה p ראשונית. נניח שידוע של $f(x)$ בדיוק שני שורשים מרוכבים אמיתיים (כלומר ב $\mathbb{C}-\mathbb{R}$). יהי E/\mathbb{Q} שדה פיצול של $f(x)$. הראו ש $Gal(E/\mathbb{Q}) = S_p$.

פתרון: $p = [\mathbb{Q}(a) : \mathbb{Q}] | [E : \mathbb{Q}] = |Gal(E/\mathbb{Q})|$, לכן לפי משפט קושי קיים בחבורה מחזור מאורך p . כעת מספיק להוכיח שקיים חילוף בחבורה $Gal(E/\mathbb{Q})$. כיוון שקיימים שני שורשים מרוכבים, הם חייבים להיות צמודים מרוכבים אחד של השני. פעולת הצמדה מרוכבת היא אוטומורפיזם של E/\mathbb{Q} שמעבירה שורש מרוכב אחד לשני וקובעת את כל האחרים, ולכן זה בהכרח חילוף.

הגדרה: הרחבה E/F נקראת **פשוטה** אם $E = F(a)$.

תרגיל: הראו שכל הרחבה סופית E של שדה סופי F היא פשוטה.

פתרון: $E^* = E - \{0\}$ היא תת-חבורה סופית כפלית, ולכן ציקלית. כלומר $E^* = \langle a \rangle$, לכן בהכרח מתקיים $E = F(a)$.

שאלה: מהי דרגת הפולינום המינימלי של a מהתרגיל הקודם, כאשר $F = \mathbb{Z}_p$?

תשובה: השדה הסופי הוא בהכרח מסדר $n = p^t$, ולכן דרגת ההרחבה $[E:F] = [F(a):F] = t$ ולכן בהכרח הפולינום המינימלי של a הוא מדרגה t .

מסקנה: כיוון שקיים שדה סופי מגודל $n = p^t$ אזי קיים פולינום אי-פריק מכל דרגה מעל $F = \mathbb{Z}_p$.

תרגיל: בהנתן פולינום אי-פריק מדרגה t מעל \mathbb{Z}_p , ושורש a של הפולינום, מיהם כל שרשי הפולינום?

פתרון: אוטומורפיזם פרובניוס $\phi: x \mapsto x^p$ הוא יוצר של חבורת גלואה של כל הרחבה סופית E/\mathbb{Z}_p . שרשי הפולינום, $\phi(a) = a^p, \phi^2(a) = a^{p^2}, \dots, \phi^{t-1}(a) = a^{p^{t-1}}$. כולם בהכרח שונים כי החבורה פועלת טרנזיטיבית על שרשי הפולינום, ולכן כל השורשים נמצאים ברשימה, אבל יש p שורשים שונים, ולכן אלה כולם).

תרגיל: הוכיחו או הפריכו: $E = \mathbb{Z}_p[a] \Rightarrow E^* = \langle a \rangle$.

פתרון: נפריך. ניקח $f(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$. בדקו שהפולינום אי-פריק. ההרחבה $\mathbb{Z}_2[a]$ היא מדרגה 4 לכל שורש a של הפולינום, לכן מדובר בשדה איזומורפי ל- \mathbb{F}_{16} , ומתקיים $\mathbb{F}_{16}^* \cong \mathbb{Z}_{15}$, אבל שורש של הפולינום $f(x)$ מקיים $a^5 = 1$ ולכן הוא לא יוצר של החבורה. אם a שורש אזי $a, a^2, a^4, a^8 = a^3$ הם כל שרשי הפולינום.

תרגיל: בנו את השדה \mathbb{F}_{32} .

פתרון: נמצא פולינום ממעלה 5 מעל \mathbb{F}_2 . הפולינומים $x, x+1, x^2+x+1$ הם הפולינומים האי-פריקים היחידים ממעלה 2 או פחות מעל \mathbb{F}_2 (בדקו!). נגדיר $f(x) = x^2(x+1)(x^2+x+1) + 1$. אזי $x^2(x^3+1) + 1 = x^5 + x^2 + 1$ לא מתחלק באף אחד מהפולינומים $x, x+1, x^2+x+1$ ולכן אי פריק (אחרת הוא היה צריך להתחלק בראשוני ממעלה 2 או פחות). מכאן נובע ש- $E = \mathbb{F}_2[x]/\langle x^5 + x^2 + 1 \rangle$ הוא שדה ממימד 5 מעל \mathbb{F}_2 ולכן $|E| = 2^{[E:\mathbb{F}_2]} = 2^5 = 32$. סיימו.