1. יהי F שדה ממאפיין p. הראו שהפולינום $f(x)=x^p-x-a$ אי-פריק אם ורק אם אין לו שורש ב F.

פתרון: ברור שאם הפולינום אי-פריק אז אין לו שורש (תמיד נכון).

נניח שאין לפולינום שורש ב F: נניח ש α שורש של הפולינום $f(x)$. אזי $\alpha,\alpha+1,\alpha+2,...,\alpha+p-1$ הם כל שורשי הפולינום: זאת כיוון ש $(\alpha+i)^p-(\alpha+i)-a=\alpha^p+i-\alpha-i-a=\alpha^p-\alpha-a=0$ (השיוויון הראשון משמאל נובע מהבינום של ניוטון, משפט פרמה והמאפיין). אם כך הוספת כל שורש לשדה F תיתן לנו שדה פיצול $E=F(\alpha)$. אם כך כיוון ש $\alpha\notin F$ נקבל ש $1<\deg(m_\alpha)\le p$, ומתקיים $m_\alpha \mid f(x)$. לפולינום $f(x)$ יש p שורשים שונים, ולכן הוא ספרבילי, ואם כך גם m_α ספרבילי, לכן $\left|Gal(E/F)\right|=[E:F]=[F(\alpha):F]=\deg(m_\alpha)>1$. לכן קיים אוטומורפיזם $\sigma\in Gal(E/F)$ המקיים $\sigma(\alpha)=\alpha+i$ עבור $1\le i\le p-1$. כעת קל לראות ש $o(\sigma)=p$ כיוון ש $\sigma^k(\alpha)=\alpha+ik$ ולא ייתכן ש $p\mid ik$ עבור $k<p$. אם כך $\deg(m_\alpha)=\left|Gal(E/F)\right|\ge p$, ולכן $m_\alpha(x)=f(x)$ כלומר בהכרח $f(x)$ אי-פריק.

2. הראו ששדה F ממאפיין $p>0$ הוא מושלם אם ורק אם לכל איבר $a\in F$ יש שורש p-י ב F.

פתרון: אם קיים איבר $a\in F$ שאין לו שורש p-י ב F אזי $f(x)=x^p-a$ הוא פולינום ללא שורש ב F. יהי α שורש של $f(x)$ בשדה הרחבה. אזי $f(x)=(x-\alpha)^p$ (בדקו זאת). הפול' המינימלי m_α מחלק את $f(x)$ ולכן הוא אי-פריק אך אינו ספרבילי, כי דרגתו גדולה מ 1, אבל כל השורשים שלו זהים. אם לכל איבר $a\in F$ יש שורש p-י ב F, יהי $f(x)$ פולינום אי-פריק אי-ספרבילי. בהכרח מתקיים $f'(x)=0$ אחרת $(f(x),f'(x))=1$ ואז הפולינום ספרבילי, סתירה. לכן בהכרח הפולינום הוא מהצורה $f(x)=a_0x^{p^k}+a_1x^{p^{k-1}}+....+a_k$. לכל $0\le i\le k$ קיים $b_i^{\,p}=a_i$ ואז $f(x)=(b_0x^{p^{k-1}}+...+b_k)^p$ בסתירה לכך שהוא אי-פריק.

3. יהי $f(x)\in\mathbb{Q}[x]$ פולינום אי-פריק מדרגה 3, ויהי $E/\mathbb{Q}$ שדה הפיצול שלו. הראו שאם יש ל $f(x)$ שורש $\alpha\in\mathbb{C}-\mathbb{R}$ אזי $Gal(E/\mathbb{Q})=S_3$.

פתרון: שאם יש ל $f(x)$ שורש $\alpha\in\mathbb{C}-\mathbb{R}$ אזי $\bar\alpha$ הצמוד המרוכב של α (שבהכרח שונה ממנו) הוא גם שורש של $f(x)$, כי $f(\bar\alpha)=\overline{f(\alpha)}=\bar 0=0$. אם כך $\bar\alpha\in E$. כעת $g(x)=(x-\alpha)(x-\bar\alpha)=x^2-(\alpha+\bar\alpha)x+\alpha\bar\alpha=x^2-2\,\mathrm{Re}(\alpha)x+|\alpha|^2\in\mathbb{R}[x]$. אם כך השורש השלישי של $f(x)$ הוא ממשי כי $\frac{f(x)}{g(x)}=x-\beta\in\mathbb{R}[x]$. לכן מתקיים $F=\mathbb{Q}(\beta)\subset\mathbb{R}$ היא הרחבה מדרגה 3 אך אינה מכילה את השורשים $\alpha,\bar\alpha$. אם כך $g(x)$ אי-פריק מעל F והרחבה ע"י α היא מדרגה 2, וסה"כ נקבל לפי כפליות דרגה ש $[E:\mathbb{Q}]=6$. כיוון ש $Gal(E/\mathbb{Q})\le S_3$ נקבל בהכרח שיוויון.

4. הראו שאם $\rho_n \in F$ שורש יחידה n-י פרימיטיבי של היחידה, אזי חבורת גלואה של שדה הפיצול של פולינום $x^n - a \in F[x]$ היא חבורה ציקלית מסדר המחלק את n.

פתרון: אם $\alpha \in E \supseteq F$ הוא שורש של $f(x) = x^n - a$, אזי השורשים של $f(x)$ הם $\alpha, \rho_n\alpha, ..., \rho_n^{n-1}\alpha \in F(\alpha) \subseteq E$. לכן $F(\alpha)$ שדה הפיצול של $f(x)$ מעל F. כל השורשים שונים ולכן $f(x)$ ספרבילי. כל אוטומורפיזם $\sigma \in Gal(F(\alpha)/F)$ נקבע ע"י תמונת α, ותמונה זאת חייבת להיות מהצורה $\sigma(\alpha) = \rho_n^{\,i}\alpha$ עבור $0 \le i \le n-1$. נגדיר העתקה $\Phi : Gal(F(\alpha)/F) \to \mathbb{Z}_n$, ע"י $\Phi : \sigma \mapsto i$, כאשר i הנ"ל. זהו הומומורפיזם חח"ע (נראה זאת בסוף), ולכן נקבל ש $Gal(F(\alpha)/F)$ איזומורפית לתת-חבורה של $\mathbb{Z}_n$ ולכן ציקלית.

נראה Φ הומ' חח"ע: אם $\Phi(\sigma) = 0$ אזי $\sigma(\alpha) = \alpha$ ולכן $\sigma = id$. נראה כפליות: אם $\sigma(\alpha) = \rho_n^i\alpha, \tau(\alpha) = \rho_n^j\alpha$ אזי $\tau\rho(\alpha) = \rho_n^{i+j}\alpha$ ולכן $\Phi(\tau\sigma) = i + j$ וגם $\Phi(\tau) + \Phi(\alpha) = i + j$ כנדרש.

5. א. בהנתן שדות $B, C \subseteq E$ נגדיר את הקומפוזיטום שלהם $B \vee C$ להיות החיתוך של כל השדות ב E המכילים את B, C. הראו שאם $a_1, ..., a_n \in E \supseteq F$ אזי $F(a_1) \vee ... \vee F(a_n) = F(a_1, ..., a_n)$.

ב. אם $F \subseteq B_1 \subseteq E$ שדות, כך ש E שדה פיצול של פולינום אי-פריק $f(x) \in F[x]$ וגם B_1 מכיל שורש של $f(x)$ אזי קיימים שדות איזומורפיים מעל F (כלומר שהאיזומורפיזמים קובעים את F) $B_1, ..., B_n$ כך ש $E = B_1 \vee ... \vee B_n$.

פתרון:

א. נובע ישירות מהגדרת $F(a_1, ..., a_n)$ כשדה הקטן ביותר המכיל את $a_1, ..., a_n$ (כלומר החיתוך של השדות המכילים את $a_1, ..., a_n$).

ב. אם $a_1, ..., a_n$ שורשים של $f(x)$ אזי חבורת גלואה פועלת עליהם טרנזיטיבית, כלומר קיים $\sigma \in Gal(E/F)$ כך ש $\sigma_i(a_1) = a_i$ לכל $1 \le i \le n$. נצמצם $\tau_i = \sigma_i|_{B_1}$ ונגדיר $B_i = \tau_i(B_1)$. מתקיים $a_i \in B_i \subseteq E$, ולכן $B_1 \vee ... \vee B_n \supseteq F(a_1) \vee ... \vee F(a_n) = F(a_1, ..., a_n) = E$.

6. יהי $F = \mathbb{Z}_p(t)$. הראו שהפולינום $f(x) = x^p - t$ אי-פריק (ללא שימוש בהכללה של משפט איזנשטיין, ואם אתם משתמשים בטיעון שאין איבר $q \in F$ כך ש $q^p = t$, יש להוכיח זאת). מצאו שדה פיצול E/F של $f(x)$ וחשבו את דרגת ההרחבה. חשבו את $Gal(E/F)$.

פתרון: נניח תחילה שאין ל $f(x)$ שורשים ב F. אם $\alpha \notin F$ שורש של הפולינום $f(x)$ אזי $f(x) = (x - \alpha)^p$ לפי הבינום של ניוטון ומאפיין השדה, והעובדה ש $\alpha^p - t = 0$; כלומר לפולינום יש שורש יחיד. כעת יהי m_α הפול' המינימלי של α. אבל $f(x) = m_\alpha(x) \cdot g(x)$ בהכרח שורש של $g(x)$. לכן נקבל $m_\alpha \mid g(x)$. לכן באינדוקציה ניתן להוכיח ש $f(x) = m_\alpha^{\,k}(x)$. אבל אז $p = \deg(f) = k \cdot \deg(m_\alpha)$. כיוון ש $\alpha \notin F$ נקבל $\deg(m_\alpha) > 1$ ואז בהכרח $\deg(m_\alpha) = p$, כלומר $f(x) = m_\alpha(x)$ ולכן $f(x)$ אי-פריק.