Алгебра 3, Септембар 2014. *19. септембар 2014.*

1. Нека је $F = \mathbb{Q}(\sqrt[4]{2}, \varepsilon_8)$. Одредити сва међупоља раширења $F/\mathbb{Q}$.

Решење. Како је $\varepsilon_8 = (\sqrt{2} + i\sqrt{2})/2$, јасно је да је $F = \mathbb{Q}(\sqrt[4]{2}, i)$, одакле је лако $|F : \mathbb{Q}| = 8$. Такође је очигледно да је F коренско поље полинома $X^4 - 2$, одакле следи да је $F/\mathbb{Q}$ Галоаово раширење. Према теореми коресподенције, тражена међупоља су тачно фиксна поља подгрупа $\mathrm{Gal}(F/\mathbb{Q})$. Одредимо $\mathrm{Gal}(F/\mathbb{Q})$.

Аутоморфизми из $\mathrm{Gal}(F/\mathbb{Q})$ су одређени сликама $\sqrt[4]{2}$ и i, при чему се они могу сликати у корен свог минималног полинома над $\mathbb{Q}$. Дакле, могуће слике од $\sqrt[4]{2}$ су $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$, а могуће слике од i су $\pm i$. Дакле, имамо осам могућности: f_{jk}, $0 \le j < 4$, $0 \le k < 2$, где $f_{jk} : \sqrt[4]{2} \mapsto i^j \sqrt[4]{2}$ и $f_{jk} : i \mapsto (-1)^k i$. Како је $|\mathrm{Gal}(F/\mathbb{Q})| = |F : \mathbb{Q}| = 8$, закључујемо да је $\mathrm{Gal}(F/\mathbb{Q}) = \{f_{jk} \mid 0 \le j < 4,\ 0 \le k < 2\}$. Такође, како је $\mathrm{Gal}(F/\mathbb{Q}) \le \mathbb{S}_4$, јер је F коренско поље полинома $X^4 - 2$, директно можемо да закључимо да је $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{D}_4$. Све битне информације о аутоморфизмима, које се добијају лаким рачуном, су дате у табели:

	$\sqrt[4]{2}$	i	ред	у $\mathbb{D}_4$	$\sqrt{2}$	$i\sqrt{2}$	$i\sqrt[4]{2}$
f_{00}	$\sqrt[4]{2}$	i	1	ε	$\sqrt{2}$	$i\sqrt{2}$	$i\sqrt[4]{2}$
f_{10}	$i\sqrt[4]{2}$	i	4	ρ	$-\sqrt{2}$	$-i\sqrt{2}$	$-\sqrt[4]{2}$
f_{20}	$-\sqrt[4]{2}$	i	2	ρ^2	$\sqrt{2}$	$i\sqrt{2}$	$-i\sqrt[4]{2}$
f_{30}	$-i\sqrt[4]{2}$	i	4	ρ^3	$-\sqrt{2}$	$-i\sqrt{2}$	$\sqrt[4]{2}$
f_{01}	$\sqrt[4]{2}$	$-i$	2	σ	$\sqrt{2}$	$-i\sqrt{2}$	$-i\sqrt[4]{2}$
f_{11}	$i\sqrt[4]{2}$	$-i$	2	$\sigma\rho^3$	$-\sqrt{2}$	$i\sqrt{2}$	$\sqrt[4]{2}$
f_{21}	$-\sqrt[4]{2}$	$-i$	2	$\sigma\rho^2$	$\sqrt{2}$	$-i\sqrt{2}$	$i\sqrt[4]{2}$
f_{31}	$-i\sqrt[4]{2}$	$-i$	2	$\sigma\rho$	$-\sqrt{2}$	$i\sqrt{2}$	$-\sqrt[4]{2}$

Дијаграм подгрупа од $\mathbb{D}_4$ је:

$$\begin{tikzcd}
 & & \langle\varepsilon\rangle \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\langle\sigma\rangle \arrow[dr] & \langle\sigma\rho^2\rangle \arrow[d] & \langle\rho^2\rangle \arrow[dl] \arrow[d] \arrow[dr] & \langle\sigma\rho\rangle \arrow[d] & \langle\sigma\rho^3\rangle \arrow[dl] \\
 & \langle\sigma,\rho^2\rangle \arrow[dr] & \langle\rho\rangle \arrow[d] & \langle\sigma\rho,\rho^2\rangle \arrow[dl] & \\
 & & \mathbb{D}_4 & &
\end{tikzcd}$$

Лако се види да су фиксна поља подгрупа $\langle\sigma, \rho^2, \rangle$, $\langle\rho\rangle$ и $\langle\sigma\rho, \rho^2\rangle$ редом $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ и $\mathbb{Q}(i\sqrt{2})$, као и да су фиксна поља подгрупа $\langle\sigma\rangle$, $\langle\sigma\rho^2\rangle$ и $\langle\rho^2\rangle$ редом $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(i\sqrt[4]{2})$ и $\mathbb{Q}(\sqrt{2}, i)$. Да бисмо одредили фиксна поља подгрупа $\langle\sigma\rho\rangle$ и $\langle\sigma\rho^3\rangle$, приметимо да је $\{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{2}^3, i, i\sqrt[4]{2}, i\sqrt{2}, i\sqrt[4]{2}^3\}$ база за F над $\mathbb{Q}$. Запишимо $x \in F$ у овој бази: $x = a_1 + a_2\sqrt[4]{2} + a_3\sqrt{2} + a_4\sqrt[4]{2}^3 + a_5 i + a_6 i\sqrt[4]{2} + a_7 i\sqrt{2} + a_8 i\sqrt[4]{2}^3$. Сада је $\sigma\rho(x) = a_1 - a_2 i\sqrt[4]{2} - a_3\sqrt{2} + a_4 i\sqrt[4]{2}^3 - a_5 i - a_6\sqrt[4]{2} + a_7 i\sqrt{2} + a_8\sqrt[4]{2}^3$. $x \in F^{\langle\sigma\rho\rangle}$ акко $\sigma\rho(x) = x$ акко $a_2 = -a_6$, $a_3 = 0$, $a_4 = a_8$, $a_5 = 0$. Дакле, фиксно поље подгрупе $\langle\sigma\rho\rangle$ чине елементи $x = a + b\sqrt[4]{2}(1-i) + ci\sqrt{2} + d\sqrt[4]{2}^3(1+i)$, $a, b, c, d \in \mathbb{Q}$. Сада није тешко видети да је фиксно поље подгрупе $\langle\sigma\rho\rangle$ једнако $\mathbb{Q}(\sqrt[4]{2}(1-i))$. Слично, фиксно поље подгрупе $\langle\sigma\rho^3\rangle$ је $\mathbb{Q}(\sqrt[4]{2}(1+i))$.

Дијаграм поља је:

$$\begin{tikzcd}
 & & F & & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[urr] & \mathbb{Q}(i\sqrt[4]{2}) \arrow[ur] & \mathbb{Q}(\sqrt{2}, i) \arrow[u] & \mathbb{Q}(\sqrt[4]{2}(1-i)) \arrow[ul] & \mathbb{Q}(\sqrt[4]{2}(1+i)) \arrow[ull] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[ul] \arrow[u] \arrow[ur] & \mathbb{Q}(i) \arrow[u] & \mathbb{Q}(i\sqrt{2}) \arrow[ul] \arrow[u] \arrow[ur] & \\
 & & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}$$

□

2. Нека је $\mathbb{C}(\omega)$ поље рационалних функција по неодређеној ω над $\mathbb{C}$. Са $f : \omega \mapsto -\omega$ и $g : \omega \mapsto \frac{1}{\omega}$ су одређени аутоморфизми из $\mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(\omega))$. Одредити фиксно поље $k = \mathbb{C}(\omega)^{\langle f,g\rangle}$ и сва међупоља раширења $\mathbb{C}(\omega)/k$.

   Решење. Приметимо најпре да $\mathbb{C}(\omega^2) \leq \mathbb{C}(\omega)^{\langle f\rangle} \lneq \mathbb{C}(\omega)$, јер $f(\omega^2) = \omega^2$. Знамо са вежби да је $|\mathbb{C}(\omega) : \mathbb{C}(\omega^2)| = 2$, па из претходног ланца видимо да је $\mathbb{C}(\omega)^{\langle f\rangle} = \mathbb{C}(\omega^2)$. Аналогно закључујемо да је $\mathbb{C}(\omega)^{\langle g\rangle} = \mathbb{C}(\omega + 1/\omega)$.

   Приметимо да $\omega^2 + 1/\omega^2 \in \mathbb{C}(\omega)^{\langle f,g\rangle}$ и уочимо ланац $\mathbb{C}(\omega^2 + 1/\omega^2) \leq \mathbb{C}(\omega)^{\langle f,g\rangle} \lneq \mathbb{C}(\omega)^{\langle f\rangle} = \mathbb{C}(\omega^2) \lneq \mathbb{C}(\omega)$. Како је $\omega^2 + 1/\omega^2 = (\omega^4 + 1)/\omega^2$ и како су $\omega^4 + 1$ и ω^2 узајамно прости, закључујемо да је $|\mathbb{C}(\omega) : \mathbb{C}(\omega^2 + 1/\omega^2)| = 4$. Из уоченог ланца сада следи да је $\mathbb{C}(\omega)^{\langle f,g\rangle} = \mathbb{C}(\omega^2 + 1/\omega^2)$.

   Приметимо да је $\mathbb{C}(\omega)/\mathbb{C}(\omega^2 + 1/\omega^2)$ Галоаово раширење (као коренско раширење полинома $X^4 - (\omega^2 + 1/\omega^2)X^2 + 1$ над $\mathbb{C}(\omega^2 + 1/\omega^2)$), па је $\mathrm{Gal}(\mathbb{C}(\omega)/\mathbb{C}(\omega^2 + 1/\omega^2)) = \langle f, g\rangle$. Међупоља одговарају подгрупама оф $\langle f, g\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, а то су $\langle f\rangle$, $\langle g\rangle$ и $\langle fg\rangle$. Прва два међупоља смо израчунали, а аналогно том рачуну добијамо да је $\mathbb{C}(\omega)^{\langle fg\rangle} = \mathbb{C}(\omega - 1/\omega)$. □

3. Испитати решивост у радикалима једначине $X^5 - 7X^2 + 7 = 0$.

   Решење. Означимо $f(X) = X^5 - 7X^2 + 7$. Овај полином је несводљив по Ајзенштајновом критеријуму, па је и сепарабилан. Посматрајући $\mathrm{Gal}(f/\mathbb{Q})$ као подгрупу од $\mathbb{S}_5$, из несводљивости можемо закључити (на стандардан начин) да $\mathrm{Gal}(f/\mathbb{Q})$ садржи 5-цикл.

   Лако је израчунати да је факторизација полинома $f(X)$ модуло 3 једнака $(X^2 + X + 2)(X^3 + 2X^2 + 2X + 2)$, па по Дедекиндовој теореми $\mathrm{Gal}(f/\mathbb{Q})$ садржи пермутацију типа $(2, 3)$. Њен трећи степен је транспозиција. Према томе $\mathrm{Gal}(f/\mathbb{Q})$ садржи 5-цикл и транспозицију, одакле је $\mathrm{Gal}(f/\mathbb{Q}) = \mathbb{S}_5$ и $f(X) = 0$ није решива у радикалима. □

4. Нека је p прост број, k поље и a елемент поља k. Претпоставимо да је полином $X^p - a$ сводљив над k. Доказати да $X^p - a$ има корен у k.

   Решење. Ако је $\mathrm{char}(k) = p$, и ако је b један корен датог полинома у k^a, тада је $X^p - a = X^p - b^p = (X - b)^p$, тј. b је једини корен од $X^p - 1$ вишеструкости p. Доказаћемо да $b \in k$. Услов да је $X^p - a = (X - b)^p$ сводљив над k нам каже да за неко $1 \leq n < p$ имамо $(X - b)^n \in k[X]$. Специјално, најмлађи коефицијент тог полинома, до на $\pm$ једнак b^n, припада k. Како су $(p, n) = 1$, то постоје $u, v \in \mathbb{Z}$ такви да $up + vn = 1$, па имамо да је $b = b^{up+vn} = (b^p)^u(b^n)^v \in k$, што смо и желели.

   Претпоставимо сада да је $\mathrm{char}(k) \neq p$ и нека је поново b један корен датог полинома у k^a. Како је $\mathrm{char}(k) \neq p$, то је полином $X^p - 1$ сепарабилан. Означимо са $1 = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ његове корене; они очигледно чине групу у односу на множење, и како је она реда p, мора бити циклична. Нека је ε неки њен генератор; тада су $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$ сви корени полинома $X^p - 1$. Одатле су $b, \varepsilon b, \varepsilon^2 b, \ldots, \varepsilon^{p-1} b$ сви корени полинома $X^p - a$, тј. $X^p - a = \prod_{i=0}^{p-1}(X - \varepsilon^i b)$.

   Сада поступамо као у првом делу задатка. Како је $X^p - a$ сводљив над k, то за неке $i_1, \ldots, i_n$, $1 \leq n < p$, имамо $(X - \varepsilon^{i_1} b) \cdot \ldots \cdot (X - \varepsilon^{i_n} b) \in k[X]$. Специјално, најмлађи коефицијент овог полинома припада k. Он је, до на $\pm$, једнак $\varepsilon^i b^n$, где је $i = i_1 + \ldots + i_n$. Како су $(p, n) = 1$, то постоје $u, v \in \mathbb{Z}$ такви да $up + vn = 1$. Приметимо да је одавде $ivn = i \mod p$, тј. $\varepsilon^{ivn} = \varepsilon^i$, па имамо да је $\varepsilon^{iv}b = (\varepsilon^{iv}b)^{up+vn} = (\varepsilon^{ivp}b^p)^u(\varepsilon^{ivn}b^n)^v = a^u(\varepsilon^i b^n)^v \in k$. Дакле, корен $\varepsilon^{iv}b$ од $X^p - a$ припада k. $\square$

5. Нека је $f : \mathbb{A}^n_{\mathbb{C}} \longrightarrow \mathbb{A}^m_{\mathbb{C}}$ полиномно пресликавање, тј. облика $f(\mathbf{x}) = (f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_m(\mathbf{x}))$, за $\mathbf{x} \in \mathbb{A}^n_{\mathbb{C}}$, где су $f_1, f_2, \ldots, f_m$ полиноми по n неодређених. Да ли су следећа тврђења тачна или не (дати доказе или контрапримере):

(1) За сваки афини алгебарски скуп $Y \subseteq \mathbb{A}^n_{\mathbb{C}}$ је његова слика $f(Y) \subseteq \mathbb{A}^m_{\mathbb{C}}$ један афини алгебарски скуп.

(2) За сваки афини алгебарски скуп $Y \subseteq \mathbb{A}^m_{\mathbb{C}}$ је његова инверзна слика $f^{-1}(Y) \subseteq \mathbb{A}^n_{\mathbb{C}}$ један афини алгебарски скуп.

(3) Ако је $Y \subseteq \mathbb{A}^n_{\mathbb{C}}$ произвољни афини алгебарски скуп, онда је његов граф при пресликавању f, дефинисан као
$$\Gamma := \{(\mathbf{x}, f(\mathbf{x})) \mid \mathbf{x} \in Y\} \subseteq \mathbb{A}^{n+m}_{\mathbb{C}},$$
један афини алгебарски скуп.

Решење. (1) Није тачно. Нпр. за $n = 2$, $m = 1$, $f : \mathbb{A}^2_{\mathbb{C}} \longrightarrow \mathbb{A}_{\mathbb{C}}$ дефинисану са $f(x_1, x_2) = x_1$ и скуп $Y = Z(X_1X_2 - 1)$ имамо да је $f(Y) = \{t \mid t \neq 0\}$, што није афини алгебарски скуп.

(2) Нека је $Y = Z(g_1, \ldots, g_k)$. Тада је $f^{-1}(Y) = \{\mathbf{x} \mid f(\mathbf{x}) \in Y\} = \{\mathbf{x} \mid (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})) \in Y\} = \{\mathbf{x} \mid g_1(f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})) = 0, \ldots, g_k(f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})) = 0\}$, па је $f^{-1}(Y)$ афини алгебарски скуп у $\mathbb{A}^n_{\mathbb{C}}$ дефинисан полиномима $g_1(f_1, \ldots, f_m), \ldots, g_k(f_1, \ldots, f_m)$.

(3) Уочимо полиномно пресликавање $(f, \mathbf{1}) : \mathbb{A}^n_{\mathbb{C}} \times \mathbb{A}^m_{\mathbb{C}} \longrightarrow \mathbb{A}^m_{\mathbb{C}} \times \mathbb{A}^m_{\mathbb{C}}$ (дефинисано на очигледан начин) и скуп $\Delta = \{(\mathbf{y}, \mathbf{y}) \mid \in \mathbb{A}^m_{\mathbb{C}}\} \subseteq \mathbb{A}^m_{\mathbb{C}} \times \mathbb{A}^m_{\mathbb{C}}$. $\Delta = Z(X_1 - X_{m+1}, X_2 - X_{m+2}, \ldots, X_m - X_{2m})$ је афини алгебарски скуп и $(f, \mathbf{1})^{-1}(\Delta) = \{(\mathbf{x}, \mathbf{x}') \mid \mathbf{x} \in \mathbb{A}^n_{\mathbb{C}}, \mathbf{x}' \in \mathbb{A}^m_{\mathbb{C}}, f(\mathbf{x}) = \mathbf{x}'\} = \{(\mathbf{x}, f(\mathbf{x})) \mid \mathbf{x} \in \mathbb{A}^n_{\mathbb{C}}\}$ је афини алгебарски скуп у $\mathbb{A}^n_{\mathbb{C}} \times \mathbb{A}^m_{\mathbb{C}}$ према (2).

Такође, како је Y афини алгебарски скуп у $\mathbb{A}^n_{\mathbb{C}}$, тада је и $Y \times \mathbb{A}^m_{\mathbb{C}}$ афини алгебарски скуп у $\mathbb{A}^n_{\mathbb{C}} \times \mathbb{A}^m_{\mathbb{C}}$ (дефинисан истим полиномима). Сада је и $(f, \mathbf{1})^{-1}(\Delta) \cap (Y \times \mathbb{A}^m_{\mathbb{C}}) = \Gamma$ афини алгебарски скуп у $\mathbb{A}^n_{\mathbb{C}} \times \mathbb{A}^m_{\mathbb{C}}$. $\square$