Алгебра 3, Јун 2014.

26. јун 2014.

1. Нека је F коренско поље полинома $(X^3-2)(X^3-3)$ над $\mathbb{Q}$. Доказати да је $\mathbb{Q}(\varepsilon_3) \leq F$ и одредити сва међупоља тог раширења.

   Решење. Корени датог полинома су $\sqrt[3]{2}, \varepsilon_3\sqrt[3]{2}, \varepsilon_3^2\sqrt[3]{2}, \sqrt[3]{3}, \varepsilon_3\sqrt[3]{3}, \varepsilon_3^2\sqrt[3]{3}$, па је $F = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}.\varepsilon_3)$, одакле је $\mathbb{Q}(\varepsilon_3) \leq F$. Како је $F/\mathbb{Q}$ Галоаово, то је и $F/\mathbb{Q}(\varepsilon_3)$ Галоаово, па су сва тражена међу поља фиксна поља подгрупа групе $\mathrm{Gal}(F/\mathbb{Q}(\varepsilon_3))$. Одредимо ову групу.

   Докажимо да је $|\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}| = 9$, па како је $|\mathbb{Q}(\varepsilon_3) : \mathbb{Q}| = 2$ и како су $(2,9) = 1$, добијамо $|F : \mathbb{Q}| = 18$, па и $|F : \mathbb{Q}(\varepsilon_3)| = 9$. Имамо $|\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}| = |\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})| \cdot |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3 \cdot |\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{2})|$. Довољно је доказати да је $X^3 - 3$ несводљив над $\mathbb{Q}(\sqrt[3]{2})$. У супротном има линеаран фактор над $\mathbb{Q}(\sqrt[3]{2})$, тј. неки његов корен припада $\mathbb{Q}(\sqrt[3]{2})$. Како је $\mathbb{Q}(\sqrt[3]{2})$ реално поље, закључујемо $\sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{2})$. Запишимо $\sqrt[3]{3}$ у бази $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ над $\mathbb{Q}$: $\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. Тада је $\sqrt[3]{3} - a = b\sqrt[3]{2} + c\sqrt[3]{4}$, па дизањем на трећи степен добијамо

   $$3 - 3a\sqrt[3]{9} + 3a^2\sqrt[3]{3} - a^3 = 2b^3 + 6bc(b\sqrt[3]{2} + c\sqrt[3]{4}) + 4c^3 = 2b^3 + 6bc(\sqrt[3]{3} - a) + 4c^3,$$

   па користећи линеарну независност $\{1, \sqrt[3]{3}, \sqrt[3]{9}\}$ над $\mathbb{Q}$ добијамо: $3 - a^3 = 2b^3 + 4c^3 - 6abc$, $3a^2 = 6bc$ и $-3a = 0$. Одавде је $a = 0$, па је $bc = 0$ и $3 = 2b^3 + 4c^3$. Ако је $b = 0$, тада је $3/4$ трећи степен рационалног броја, а ако је $c = 0$ тада је $3/2$ трећи степен рационалног броја. Контрадикција.

   Према томе $G = \mathrm{Gal}(F/\mathbb{Q}(\varepsilon_3))$ је група реда 9, дакле Абелова (групе реда p^2 су Абелове). Питање је да ли је циклична или производ две цикличне. Аутоморфизми поља F над $\mathbb{Q}(\varepsilon_3)$ су одређени сликама $\sqrt[3]{2}$ и $\sqrt[3]{3}$, коњи се сликају у корене њихових минималних полионома над $\mathbb{Q}(\varepsilon_3)$ $X^3 - 2$ и $X^3 - 3$, па како их има 9, видимо да су елементи групе G аутоморфизми f_{ij}, $0 \leq i, j < 3$, дати са:

   $$f_{ij} : \begin{cases} \sqrt[3]{2} \mapsto \varepsilon_3^i\sqrt[3]{2} \\ \sqrt[3]{3} \mapsto \varepsilon_3^j\sqrt[3]{3} \end{cases}.$$

   Како сви аутоморфизми фиксирају $\mathbb{Q}(\varepsilon_3)$, лако видимо да су сви нетривијлани аутоморфизми реда 3, па је $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Група G има четири праве нетривијалне подгрупе реда 3, и лако је видети да су то $H = \langle f_{10} \rangle$, $K = \langle f_{11} \rangle$, $L = \langle f_{12} \rangle$ и $M = \langle f_{01} \rangle$. Потребно је још одретити њихова фиксна поља.

   Најпре приметимо да је лако $F^H = \mathbb{Q}(\sqrt[3]{3}, \varepsilon_3)$ и $F^M = \mathbb{Q}(\sqrt[3]{2}, \varepsilon_3)$.

   Израчунајмо F^K. Приметимо да је $f_{11}(\sqrt[3]{2}/\sqrt[3]{3}) = \varepsilon_3\sqrt[3]{2}/\varepsilon_3\sqrt[3]{3} = \sqrt[3]{2}/\sqrt[3]{3}$, па $\mathbb{Q}(\sqrt[3]{2}/\sqrt[3]{3}, \varepsilon_3) \leq F^K$ и стандардан аргумент са степеном раширења нам даје $F^K = \mathbb{Q}(\sqrt[3]{2}/\sqrt[3]{3}, \varepsilon_3)$.

   Слично претходном пасусу имамо и $F^L = \mathbb{Q}(\sqrt[3]{2}\sqrt[3]{3}, \varepsilon_3)$. □

2. Факторисањем полинома $p(X) = X^6 - 14X^3 + 34X^2 + 59X + 15$ модуло 2, 3 и 5 доказати да једначина $p(X) = 0$ није решива у радикалима.

   Решење. Факторишимо најпре $p(X)$ модуло 2, 3 и 5.

   $p_2(X) = X^6 + X + 1$. Јасно је да $p_2(X)$ нема линеаран корен. Проверимо да ли има квадратни фактор. Означимо са $k(X)$ квадратни фактор од $p_2(X)$. Знамо да $k(X) \mid X^{2^2} - X = X(X+1)(X^2+X+1)$, па је $k(X) = X^2 + X + 1$. Лако се види да $k(X)$ не дели $p_2(X)$. Према томе, ако је $p_2(X)$ свођив, онда је производ два полинома трећег степена. Означимо са $t(X)$ фактор трећег степена од $p_2(X)$. Знамо да $t(X) \mid X^{2^3} - X = X(X^7 + 1)$. Тада $t(X) \mid X^7 + 1$ и $t(X) \mid p_2(X) \mid X^7 + X^2 + X$, па $t(X)$ дели и разлику $X^2 + X + 1$, што је контрадикција. Дакле, $p_2(X)$ је несводљив над $\mathbb{F}_2$.

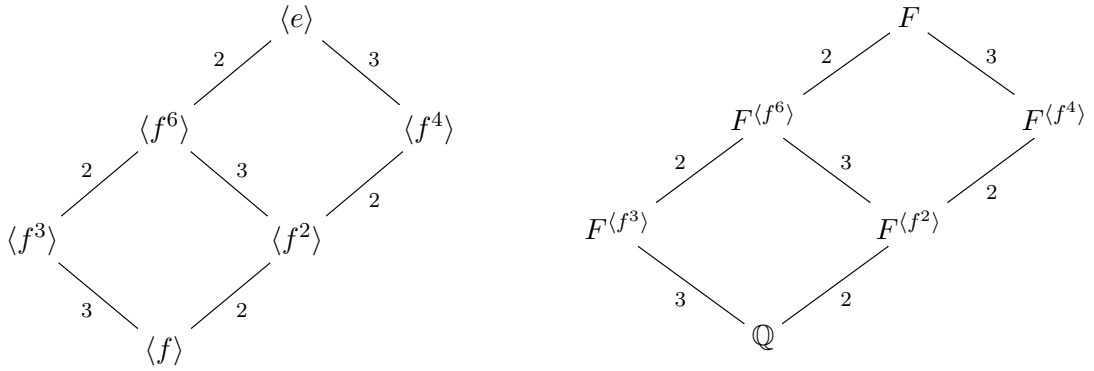
   $p_3(X) = X^6 + X^3 + X^2 - X = X(X^5 + X^2 + X - 1)$. Раставимо још $q(X) = X^5 + X^2 + X - 1$ над $\mathbb{F}_3$. Лако је видети да $q(X)$ нема линеаран фактор. Ако је сводљив, онда има квадратан фактор. Претпоставимо да је $k(X)$ његов квадратан фактор. Знамо да $k(X) \mid X^{3^2} - X = X(X^8 - 1) = X(X^4 - 1)(X^4 + 1)$. Ако $k(X) \mid X^4 - 1 \mid X^5 - X$, па дели и разлику $q(X) - X^5 + X = X^2 + 2X - 1$, тј. $k(X) = X^2 + 2X - 1$ и лако видимо да $k(X)$ не дели $q(X)$. Ако $k(X) \mid X^4 + 1 \mid X^5 - X$, дели и разлику $q(X) - X^5 - X = X^2 - 1 = (X-1)(X+1)$, што није могуће. Дакле, $q(X)$ нема ни квадратни фактор, па је несводљив.

$p_5(X) = X^6 + X^3 - X^2 - X = X(X^5 + X^2 - X - 1) = X(X-1)(X^4 + X^3 + X^2 + 2X + 1) = X(X-1)(X+1)(X^3+X+1)$. Приметимо још да је X^3+X+1 несводљив над $\mathbb{F}_5$, јер нема линеаран фактор.

Нека је $G = \mathrm{Gal}(p/\mathbb{Q})$. Како је $p_2(X)$ несводљив над $\mathbb{F}_2$, то је и $p(X)$ несводљива над $\mathbb{Z}$, па и над $\mathbb{Q}$. Специјално, $p(X)$ је сепарабилан полином и G је транзитивна подгрупа од $\mathbb{S}_6$. Како су $p_2(X)$, $p_3(X)$ и $p_5(X)$ сепарабилни можемо применити Дедекиндову теорему. Она каже да G садржи 6-цикл, 5-цикл и 3-цикл. Како је $5 > 6/2$ и 5 је прост број, имамо да је G тразитивна подгрупа од $\mathbb{S}_6$ која садржи 5-цикл и 3-цикл, па је $\mathbb{A}_6 \leq G$. Ово је већ довољно да закључимо да је G нерешива група, па је $p(X) = 0$ једначина нерешива у радикалима. Приметимо само да је $G = \mathbb{S}_6$, јер садржи непарну пермутацију (онај 6-цикл). □

3. Одредити све конструктибилне елементе у пољу $F = \mathbb{Q}(\varepsilon_{13})$.

Решење. $F/\mathbb{Q}$ је Галоаово решење и $G = \mathrm{Gal}(F)/\mathbb{Q}) \cong \mathbb{Z}/12\mathbb{Z}$. Нека је $G = \langle f \rangle$. Уочимо коресподенцију раширења $F/\mathbb{Q}$ (на првом дијаграму су означени и индекси подгрупа у одговарајућим групама, а на другом степен раширења поља над одговарајућим потпољем):



Са дијаграма је јасно да су $F^{\langle f^4 \rangle}$ конструктибилни елементи из F. Ако $a \in F^{\langle f^4 \rangle}$, тада је $\mathbb{Q}(a)$ једнако $\mathbb{Q}$, $F^{\langle f^2 \rangle}$ или $F^{\langle f^4 \rangle}$; у сваком случају постоји конструктибилни низ поља између $\mathbb{Q}$ и $\mathbb{Q}(a)$. Ако $a \notin F^{\langle f^4 \rangle}$, тада је $\mathbb{Q}(a)$ једнако $F^{\langle f^3 \rangle}$, $F^{\langle f^6 \rangle}$ или F, па је $|\mathbb{Q}(a) : \mathbb{Q}|$ једнако 3, 6 или 12; у сваком случају a није конструктибилан. □

4. Нека је k^a алгебарско затворење поља k карактеристике 0 и $f \in \mathrm{Aut}_k(k^a)$. Нека је $F = \{x \in k^a \mid f(x) = x\}$ фиксно поље аутоморфизма f. Ако је E/F коначно Галоаово раширење, доказати да је $\mathrm{Gal}(E/F) = \langle f|_E \rangle$. Доказати да је свако коначно раширење поља F циклично.

Решење. Приметимо да $f|_E$ по дефиницији фиксира F, па због нормалности E/F имамо да $f|_E \in \mathrm{Gal}(E/F)$. Доказаћемо да је $E^{\langle f|_E \rangle} = F$, одакле следи $\mathrm{Gal}(E/F) = \langle f|_E \rangle$. Тривијално $F \leq E^{\langle f|_E \rangle}$. Ако $a \in E^{\langle f|_E \rangle}$, тада $f|_E(a) = a$, па $f(a) = a$, тј. $a \in F$. Дакле, $F = E^{\langle f|_E \rangle}$.

Ако је K/F коначно раширење, уочимо његово Галоаово затворење E/F, оно је такође коначно. Како је E/F циклично према претходном, подгрупа од $\mathrm{Gal}(E/F)$ која фиксира K је нормална, па је K/F нормално, тј. Галоаово. Дакле, $K = E$ и K/F је циклично. □

5. (а) Нека је $\mathfrak{a} = \langle X^2 + Y^2 - 1, Y - 1 \rangle \subseteq \mathbb{C}[X, Y]$. Одредити бар један полином f који припада идеалу $I(Z(\mathfrak{a}))$, али не припада $\mathfrak{a}$.

(б) Скуп $M_n(\mathbb{C})$ свих $n \times n$ комплексних матрица идентификујемо са афиним n^2-простором $\mathbb{A}^{n^2}_{\mathbb{C}}$ (свакој матрици одговара једна тачка афиног простора). Доказати да је скуп свих оваквих матрица које имају бар једну вишеструку сопствену вредност један алгебарски (тј. Зариски затворен) скуп у $\mathbb{A}^{n^2}_{\mathbb{C}}$.

(в) Да ли је скуп матрица из $M_n(\mathbb{C})$ чије су све сопствене вредности једноструке, афини алгебарски скуп у неком афином простору?

Решење. (а) Приметимо да је $\mathfrak{a} = \langle X^2, Y - 1 \rangle$, јер је $X^2 + Y^2 - 1 = X^2 + (Y+1)(Y-1)$. Према Хилбертовој теореми је $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. Јасно је да $X \in \sqrt{\mathfrak{a}}$, јер $X^2 \in \mathfrak{a}$, али такође $X \notin \mathfrak{a}$.

(б) Матрица A има вишеструку сопствену вредност акко карактеристични полином $\chi_A(t) = \det(tE - A)$ има вишеструки корен акко је дискриминанта $\Delta_t(\det(tE - A)) = 0$. Према томе, дати скуп је $Z(\Delta_t(\det(tE-(X_{ij}))))$. (Сетимо се да је $\det(tE-(X_{ij}))$ полином по t чији су коефицијенти полиноми по X_{ij}, и сетимо се да се дискриминанта полинома изражава као полином од њених коефицијената. Према томе $\Delta_t(\det(tE - (X_{ij})))$ је полином по X_{ij}.) Овде смо са X_{ij}, $1 \leq i, j \leq n$, означавали променљиве у одговарајућој $\mathbb{C}$-алгебри полинома.

(в) Матрица A има једноструке сопствене вредности акко $\Delta_t(\det(tE - A)) \neq 0$, тј. има инверз. Ако посматрамо простор $\mathbb{A}_{\mathbb{C}}^{n^2+1}$ и означимо променљиве у $\mathbb{C}$-алгебри полинома са X_{ij}, $1 \leq i, j \leq n$, и Y, тада матрице са једноструким сопственим вредностима на очигледан начин идентификујемо са тачкама на $Z(Y \cdot \Delta_t(\det(tE - (X_{ij}))) - 1)$. □

6. Нека је A комутативни прстен са јединицом за који постоје неки његови идеали $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k$ такви да је $\bigcap_{j=1}^{k} \mathfrak{a}_j = 0$ и додатно, да су количнички прстени $A/\mathfrak{a}_j$ Нетерини, за све $1 \leq j \leq k$. Доказати да је и A Нетерин прстен.

Решење. Доказаћемо да су сви идеали коначно генерисани. Нека је $\mathfrak{a} \triangleleft A$ произвољан идеал. Означимо са $\mathfrak{b}_0 = \mathfrak{a}$, $\mathfrak{b}_i = \mathfrak{b}_{i-1} \cap \mathfrak{a}_i = \mathfrak{a} \cap \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \ldots \cap a_i$, $1 \leq i \leq k$. Приметимо $\mathfrak{a} = \mathfrak{b}_0 \supseteq \mathfrak{b}_1 \supseteq \mathfrak{b}_2 \supseteq \ldots \supseteq \mathfrak{b}_k = 0$. Идеал $\mathfrak{b}_{i-1} + \mathfrak{a}_i/\mathfrak{a}_i$ прстена $A/\mathfrak{a}_i$, за $1 \leq i \leq k$, је коначно генерисан, јер је $A/\mathfrak{a}_i$ Нетерин; нека су $x_{i1}, x_{i2}, \ldots, x_{in_i} \in \mathfrak{b}_{i-1}$ такви да $\langle x_{ij} + \mathfrak{a}_i \mid 1 \leq j \leq n_i \rangle = \mathfrak{b}_i + \mathfrak{a}_i/\mathfrak{a}_i$ у $A/\mathfrak{a}_i$. Тврдимо да је $\mathfrak{a} = \langle x_{ij} \mid 1 \leq i \leq k,\ 1 \leq j \leq n_i \rangle$. $\supseteq$ је јасно.

Нека је $y \in \mathfrak{a}$. Запишимо $y + \mathfrak{a}_1 = \sum_{j=1}^{n_1} r_{1j}x_{1j} + \mathfrak{a}_1$; тада $y_1 = y - \sum_{j=1}^{n_1} r_{1j}x_{1j} \in \mathfrak{a} \cap \mathfrak{a}_1 = \mathfrak{b}_1$. Запишимо $y_1 + \mathfrak{a}_2 = \sum_{j=1}^{n_2} r_{2j}x_{2j} + \mathfrak{a}_2$; тада $y_2 = y_1 - \sum_{j=1}^{n_2} r_{2j}x_{2j} \in \mathfrak{b}_1 \cap \mathfrak{a}_2 = \mathfrak{b}_2$. Наставимо поступак: ако имамо $y_{i-1} \in \mathfrak{b}_{i-1}$, запишимо $y_{i-1} + \mathfrak{a}_i = \sum_{j=1}^{n_i} r_{ij}x_{ij} + \mathfrak{a}_i$; тада $y_i = y_{i-1} - \sum_{j=1}^{n_i} r_{ij}x_{ij} \in \mathfrak{b}_{i-1} \cap \mathfrak{a}_i = \mathfrak{b}_i$. Коначно добијамо $y_k \in \mathfrak{b}_k = 0$, па је

$$0 = y_k = y_{k-1} - \sum_{j=1}^{n_k} r_{kj}x_{kj} = y_{k-2} - \sum_{j=1}^{n_{k-1}} r_{k-1,j}x_{k-1,j} - \sum_{j=1}^{n_k} r_{kj}x_{kj} = \ldots$$

$$= \ldots = y - \sum_{j=1}^{n_1} r_{1j}x_{1j} - \sum_{j=1}^{n_2} r_{2j}x_{2j} - \ldots - \sum_{j=1}^{n_{k-1}} r_{k-1,j}x_{k-1,j} - \sum_{j=1}^{n_k} r_{kj}x_{kj},$$

одакле $y \in \langle x_{ij} \mid 1 \leq i \leq k,\ 1 \leq j \leq n_i \rangle$. □