Алгебра 3, Јул 2014.

1. Нека је $F = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3})$. Доказати да је $F/\mathbb{Q}(\sqrt{3})$ Галоаово раширење и одредити сва међупоља раширења $F/\mathbb{Q}(\sqrt{3})$.

   Решење. Корени полинома $(X^2+1)(X^2-3)(X^3-2)$ су $\pm i$, $\pm\sqrt{3}$, $\sqrt[3]{2}$, $\varepsilon_3\sqrt[3]{3}$ и $\varepsilon_3^2\sqrt[3]{3}$. Како је $\varepsilon_3 = (-1+i\sqrt{3})/2$ видимо да је F коренско поље овог полинома, па је $F/\mathbb{Q}$ Галоаово. Одатле је и $F/\mathbb{Q}(\sqrt{3})$ Галоаово. Лако видимо да је $|\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}| = 4$ и $|\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}| = 3$. Како су $(4,3) = 1$ имамо да је $|F : \mathbb{Q}| = 12$, па како је $|\mathbb{Q}(\sqrt{3}) : \mathbb{Q}| = 2$ добијамо $|F : \mathbb{Q}(\sqrt{3})| = 6$. Дакле, $|\mathrm{Gal}(F/\mathbb{Q}(\sqrt{3}))| = 6$. Међупоља раширења $F/\mathbb{Q}(\sqrt{3})$ ћемо наћи као фиксна поља подгрупа $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{3}))$. Опишимо ближе ову групу.

   Елементи групе $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{3}))$ су одређени сликама i и $\sqrt[3]{3}$, који морају редом да се сликају у корене полинома $\mu_{i,\mathbb{Q}(\sqrt{3})}(X) = X^2+1$ и $\mu_{\sqrt[3]{3},\mathbb{Q}(\sqrt{3})}(X) = X^3-3$. Како имамо шест могућности, закључујемо да оне одређују елементе $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{3}))$. Како сваки аутоморфизам фиксира $\sqrt{3}$, користећи $\varepsilon_3 = (-1+i\sqrt{3})/2$ и $\varepsilon_3^2 = (-1-i\sqrt{3})/2$, можемо израчунати и слике од ε_3. Све ово је дато у следећој таблици. (У претпоследњој колони рачунамо ред аутоморфизама, одакле видимо да је $\mathrm{Gal}(F/\mathbb{Q}(\sqrt{3})) \cong \mathbb{D}_3$, па у последњој колони дајемо коресподенцију са $\mathbb{D}_3$.)

	i	$\sqrt[3]{3}$	ε_3	ред	у $\mathbb{D}_3$
f_1	i	$\sqrt[3]{3}$	ε_3	1	ε
f_2	$-i$	$\sqrt[3]{3}$	ε_3^2	2	σ
f_3	i	$\varepsilon_3\sqrt[3]{3}$	ε_3	3	ρ
f_4	$-i$	$\varepsilon_3\sqrt[3]{3}$	ε_3^2	2	$\sigma\rho^2$
f_5	i	$\varepsilon_3^2\sqrt[3]{3}$	ε_3	3	ρ^2
f_6	$-i$	$\varepsilon_3^2\sqrt[3]{3}$	ε_3^2	2	$\sigma\rho$

   Група $\mathbb{D}_3$ има четири праве нетривијалне подгрупе: $H = \langle\rho\rangle$, $K = \langle\sigma\rangle$, $L = \langle\sigma\rho\rangle$ и $M = \langle\sigma\rho^2\rangle$. Одрђујемо фиксна поља.

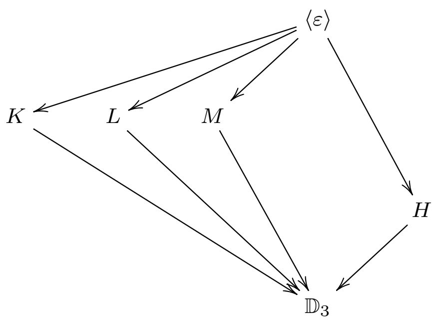
   Јасно је да $i \in F^H$, па је $\mathbb{Q}(i,\sqrt{3}) \le F^H$. Како је $|F^H : \mathbb{Q}(\sqrt{3})| = |\mathrm{Gal}(F/\mathbb{Q}(\sqrt{3})) : H| = 2$, па како је и $|\mathbb{Q}(i,\sqrt{3}) : \mathbb{Q}(\sqrt{3})| = 2$ закључујемо да је $F^H = \mathbb{Q}(i,\sqrt{3})$.

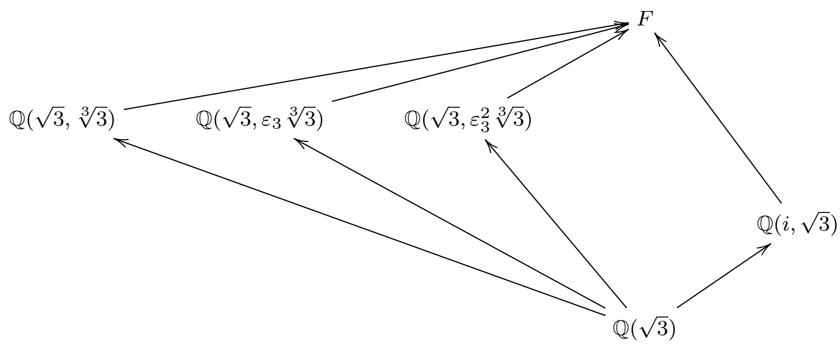
   Како $\sqrt[3]{3} \in F^K$, аналоган аргумент из претходног пасуса нам даје $F^K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$.

   Приметимо да је $\sigma\rho(\varepsilon_3\sqrt[3]{3}) = \sigma\rho(\varepsilon_3)\sigma\rho(\sqrt[3]{3}) = \varepsilon_3^2\varepsilon_3^2\sqrt[3]{3} = \varepsilon_3\sqrt[3]{3}$, па закључујемо $F^L = \mathbb{Q}(\sqrt{3}, \varepsilon_3\sqrt[3]{3})$.

   Коначно, приметимо да је $\sigma\rho^2(\varepsilon_3^2\sqrt[3]{3}) = \varepsilon_3^2\sqrt[3]{3}$, па закључујемо $F^M = \mathbb{Q}(\sqrt{3}, \varepsilon_3^2\sqrt[3]{3})$.

   Галоаова коресподенција је дата на дијаграму:





□

2. Испитати да ли је једначина $X^5 - 4X + 2 = 0$ решива у радикалима.

   Решење. Нека је $p(X) = X^5 - 4X + 2$. $p(X)$ је несводљив полином по Ајзенштајновом критеријуму, па је и сепарабилан, и $\mathrm{Gal}(p/\mathbb{Q}) \le \mathbb{S}_5$ (стандардна идентификација). Означимо са F његово коренско поље. Како је $p'(X) = 5X^4 - 4$, видимо да $p(X)$ има два локална екстремума, одакле закључујемо да $p(X)$ има највише три реална корена. Са друге стране, $\lim_{x\to-\infty} p(x) = -\infty$, $p(0) = 2 > 0$, $p(1) = -1 < 0$ и $\lim_{x\to+\infty} p(x) = +\infty$ нам каже да $p(X)$ има бар три реална корена. Дакле, $p(X)$

има тачно три реална корена, а преостала два су међусобно коњуговани комплексни бројеви. Сада нам стандардни аргумент (рађен на вежбама) даје да је $\mathrm{Gal}(p/\mathbb{Q}) = \mathbb{S}_5$, па једначина $p(X) = 0$ није решива у радикалима. $\square$

3. Нека је $p(X) = X^8 + 3X - 6$.

   1) Доказати да $p(X)$ има реалан корен α. Факторисати полином $p(X)$ модуло 2.

   2) Испитати да ли је α конструктибилан број.

   Решење. 1) Јасно је да $p(X)$ има реалан корен, јер је $p(0) = -6$ и $p(2) = 256$. Полином $p(X)$ модуло 2 је једнак $X^8 + X = X^{2^3} + X$, а знамо да је овај полином производ свих несводљивих моничних полинома степена 1 и 3. Несводљиви линеарни полиноми су X и $X + 1$, а несводљиви полиноми степена 3 су $X^3 + X^2 + 1$ и $X^3 + X + 1$ (јасно је да једино ови полиноми степена 3 немају корен у $\mathbb{F}_2$). Дакле, $p(X) \equiv X(X+1)(X^3+X^2+1)(X^3+X+1) \mod 2$.

   2) Полином $p(X)$ је несводљив по Ајзенштајновом критеријуму, па је и сепарабилан. Имамо природно утапање $\mathrm{Gal}(p/\mathbb{Q}) \leq \mathbb{S}_8$. Његова редукција модуло 2 је сепарабилна како смо видели, па по Дедекиндовој теореми можемо да закључимо да $\mathrm{Gal}(p/\mathbb{Q})$ садржи пермутацију чија је циклусна декомпозиција типа $(3, 3)$. Специјално то значи да $\mathrm{Gal}(p/\mathbb{Q})$ садржи елемент реда 3. Према томе $3 \mid |\mathrm{Gal}(p/\mathbb{Q})| = |F : \mathbb{Q}|$, где је F коренско поље полинома $p(X)$ над $\mathbb{Q}$, па $|F : \mathbb{Q}|$ није степен двојке, одакле следи да α није конструктибилан број. $\square$

4. Нека је $p(X)$ сепарабилан несводљив полином степена n над пољем k, F његово коренско поље и α један његов корен. Претпоставимо да је $\mathrm{Gal}(F/k) \cong \mathbb{S}_n$. Одредити сва међупоља раширења $k(\alpha)/k$.

   Решење. Нека су $\alpha_1, \alpha_2, \ldots, \alpha_n = \alpha$ сви корени полинома $p(X)$. Приметимо да $f \in \mathrm{Gal}(F/k)$ фиксира $k(\alpha)$ акко фиксира α. Према томе, $k(\alpha)$ је фиксо поље подгрупе $H = \{f \in \mathrm{Gal}(F/k) \mid f(\alpha) = \alpha\}$, па је питање међупоља раширења $k(\alpha)/k$ еквивалентно питању надгрупа подгрупе H.

   Претпоставимо да је $H \lneq K$ и $f \in K \smallsetminus H$. Како је $\mathrm{Gal}(F/k) \cong \mathbb{S}_n$, приметимо да H, па тиме и K, садржи све транспозиције $\lfloor \alpha_i, \alpha_j \rceil$, за $1 \leq i < j < n$. Како $f \notin H$, то је $f(\alpha_n) = \alpha_k$, за неко $k < n$. Изаберимо $l < n$, $l \neq k$ и приметимо да K садржи $f^{-1}\lfloor \alpha_l, \alpha_k \rceil f = \lfloor f^{-1}(\alpha_l), \alpha_n \rceil$, тј. K садржи транспозицију $\lfloor \alpha_m, \alpha_n \rceil$, где је $\alpha_m = f^{-1}(\alpha_l)$. Дакле, K садржи транспозиције $\lfloor \alpha_m, \alpha_i \rceil$, $1 \leq i \leq n$, $i \neq m$, а оне генеришу $\mathbb{S}_n$. Дакле, H нема правих надгрупа, па $k(\alpha)/k$ нема правих међупоља. $\square$

5. 1) Да ли је идеал $\mathfrak{a} = \langle (Z-1)^2, X^2 + XY + Y - X^2 Z \rangle \subseteq \mathbb{C}[X, Y, Z]$ радикалски? Одговор доказати/аргументовати.

   2) Доказати да је хиперповрш $F := Z(XY - Z) \subseteq \mathbb{A}^3_{\mathbb{C}}$ изоморфна афиној равни $\mathbb{A}^2_{\mathbb{C}}$. Одредити један експлицитни изоморфизам $\varphi : F \longrightarrow \mathbb{A}^2_{\mathbb{C}}$, одредити њему одговарајући хомоморфизам координатних прстена $\varphi^* : A[\mathbb{A}^2_{\mathbb{C}}] \longrightarrow A[F]$ и експлицитно описати и њихове инверзе.

   3) Да ли је хиперповрш $Z(XY - Z^2) \subseteq \mathbb{A}^3_{\mathbb{C}}$ изоморфна са $\mathbb{A}^2_{\mathbb{C}}$?

   4) Нека је L произвољна права у пројективном простору $\mathbb{P}^3_{\mathbb{C}}$. Доказати да је скуп свих правих у $\mathbb{P}^3_{\mathbb{C}}$ које *не пресецају* дату праву L параметризован (тј. у бијекцији са) једним варијететом, који је изоморфан афиној 4-равни $\mathbb{A}^4_{\mathbb{C}}$.

   Решење. 1) Приметимо да $Z - 1 \in \sqrt{\mathfrak{a}}$. Ако $Z - 1 \in \mathfrak{a}$, тада је $Z - 1 = p(X, Y, Z)(Z-1)^2 + q(X, Y, Z)(X^2 + XY + Y - X^2 Z)$. За $X = Y = 0$, добијамо једнакост у $\mathbb{C}[Z]$: $Z - 1 = p(0, 0, Z)(Z-1)^2$, па узимајући степене леве и десне стране видимо да она није могућа. Дакле, $Z - 1 \notin \mathfrak{a}$, па $\mathfrak{a}$ није радикалски.

   2) Уочимо морфизам $\varphi : F :\longrightarrow \mathbb{A}^2_{\mathbb{C}}$ дат са $\varphi(x, y, z) = (x, y)$ и морфизам $\psi : \mathbb{A}^2_{\mathbb{C}} \longrightarrow F$ дат са $\psi(x, y) = (x, y, xy)$. Очигледно је $\psi\varphi = \mathrm{id}_F$ и $\varphi\psi = \mathrm{id}_{\mathbb{A}^2_{\mathbb{C}}}$, па су F и $\mathbb{A}^2_{\mathbb{C}}$ су изоморфни.

   Лако је видети да је $XY - Z$ несводљив полином у $\mathbb{C}[XY - Z]$, па је $\langle XY - Z \rangle$ прост, тј. $I(F) = \langle XY - Z \rangle$. Према томе $A[F] = \mathbb{C}[X, Y, Z]/\langle XY - Z \rangle$. Одговарајући хомоморфизам $\varphi^* : \mathbb{C}[X, Y] = A[\mathbb{A}^2_{\mathbb{C}}] \longrightarrow A[F] = \mathbb{C}[X, Y, Z]/\langle XY - Z \rangle$ је дат са: $\varphi^* : X \mapsto X + \langle XY - Z \rangle$, $Y \mapsto Y + \langle XY - Z \rangle$. Њему одговара инверз $\psi^* : \mathbb{C}[X, Y, Z]/\langle XY - Z \rangle \longrightarrow \mathbb{C}[X, Y]$ дат са: $\psi^* : X + \langle XY - Z \rangle \mapsto X$, $Y + \langle XY - Z \rangle \mapsto Y$ и $Z + \langle XY - Z \rangle \mapsto XY$.

3) Означимо $F = Z(XY - Z^2)$. Није тешко видети да је $XY - Z^2$ несводљив у $\mathbb{C}[X,Y,Z]$, па је $\langle XY - Z^2\rangle$ прост, тј. $I(F) = \langle XY - Z^2\rangle$. Према томе, одговарајући координатни прстен је $A[F] = \mathbb{C}[X,Y,Z]/\langle XY - Z^2\rangle$. Приметимо да $A[F]$ није домен са јединственом факторизацијом ($\bar{X}\bar{Y} = \bar{Z}^2$; тривијалан рачун показује да су $\bar{X}$, $\bar{Y}$ и $\bar{Z}$ различити, неивертибилни и несводљиви елементи у $A[F]$), па према томе није изоморфан са $A[\mathbb{A}^2_{\mathbb{C}}] = \mathbb{C}[X,Y]$. Како нису изоморфни као прстени, нису изоморфни ни као $\mathbb{C}$-алгебре, па ни F и $\mathbb{A}^2_{\mathbb{C}}$ нису изоморфни.

4) Можемо да гледамо пројективну праву као пресек две пројективне равни. Пројетивна раван је описана хомогеном линеарном једначином типа: $\alpha_1X_1 + \alpha_2X_2 + \alpha_3X_3 + \alpha_4X_4 = 0$, где нису сви α_i једнаки 0. Дакле, пројективна права је одређена системом овакве две једначине:

$$\begin{aligned} \alpha_1X_1 + \alpha_2X_2 + \alpha_3X_3 + \alpha_4X_4 = 0 \\ \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 = 0, \end{aligned}$$

чији је ранг 2 (ако је ранг 1, тада ове две једначине описују исту раван). Системи датог типа су описани матрицом

$$M = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \end{bmatrix},$$

при чему та матрица представља праву акко је ранга 2, а раван акко је ранга 1. Јасно је да две овакве матрице M и N, обе ранга два, могу да одређују исту праву, што је еквивалентно са $\operatorname{rank}\begin{bmatrix} M \\ N \end{bmatrix} = 2$. Праве одређене матрицама M и N имају пресек акко $\operatorname{rank}\begin{bmatrix} M \\ N \end{bmatrix} = 3$, а немају пресек акко $\operatorname{rank}\begin{bmatrix} M \\ N \end{bmatrix} = 4$, еквивалентно $\det\begin{bmatrix} M \\ N \end{bmatrix} \neq 0$.

Без умањења општости, претпоставимо да је L дата матрицом $L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$. Тврдимо да је скуп свих правих које не секу L једнак:

$$S = \left\{ \begin{bmatrix} x & y & 1 & 0 \\ u & v & 0 & 1 \end{bmatrix} \; : \; x, y, u, v \in \mathbb{C} \right\}.$$

$\supseteq$: Ако $M \in S$, тада је $\operatorname{rank}(M) = 2$ и $\det\begin{bmatrix} L \\ M \end{bmatrix} = 1$, па права M не сече L.

$\subseteq$: Ако је права $M = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \end{bmatrix}$ не сече L, тада $\det\begin{bmatrix} L \\ M \end{bmatrix} = \alpha_3\beta_4 - \alpha_4\beta_3 \neq 0$. Како α_3 и β_3 не могу оба бити 0, до на замену врста у M, можемо претпоставити да је $\alpha_3 \neq 0$, па дељењем прве врсте са α_3 (а што је иста пројективна раван) видимо да је права M дата матрицом (опет означавамо са M, α, β, нема забуне) $M = \begin{bmatrix} \alpha_1 & \alpha_2 & 1 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \end{bmatrix}$. Када прву врсу помножимо са $-\beta_3$ и додамо другој, добијамо да је права M дата матрицом (и даље означавамо M, α, β) $M = \begin{bmatrix} \alpha_1 & \alpha_2 & 1 & \alpha_4 \\ \beta_1 & \beta_2 & 0 & \beta_4 \end{bmatrix}$. Услов да се L и M не секу сада гласи $\beta_4 \neq 0$, па поделимо другу врсту са β_4 и добијамо $M = \begin{bmatrix} \alpha_1 & \alpha_2 & 1 & \alpha_4 \\ \beta_1 & \beta_2 & 0 & 1 \end{bmatrix}$. Коначно додавањем друге врсте помножене са $-\alpha_4$ првој добијамо да је права M дата са $M = \begin{bmatrix} \alpha_1 & \alpha_2 & 1 & 0 \\ \beta_1 & \beta_2 & 0 & 1 \end{bmatrix}$, односно $M \in S$.

Даље тврдимо да су праве $M = \begin{bmatrix} x & y & 1 & 0 \\ u & v & 0 & 1 \end{bmatrix}$ и $N = \begin{bmatrix} x' & y' & 1 & 0 \\ u' & v' & 0 & 1 \end{bmatrix}$ једнаке акко $x = x', y = y', u = u', v = v'$. Заиста, ако су M и N једнаке, тада је $\operatorname{rank}\begin{bmatrix} M \\ N \end{bmatrix} = 2$, па рачуном минора $M_{11}, M_{21}, M_{31}, M_{41}$, који сви морају бити једнаки 0, добијамо жељени закључак.

Сада је $f : \mathbb{A}^4_{\mathbb{C}} \longrightarrow S$, дефинисана са $f : (x, y, u, v) \mapsto \begin{bmatrix} x & y & 1 & 0 \\ u & v & 0 & 1 \end{bmatrix}$, тражена параметризација. $\square$