Алгебра 3, Јануар 2015. *24. јануар 2015.*

1. Одредити потпоља коренског поља полинома $(X^2-2)(X^3-2)$ над $\mathbb{Q}$.

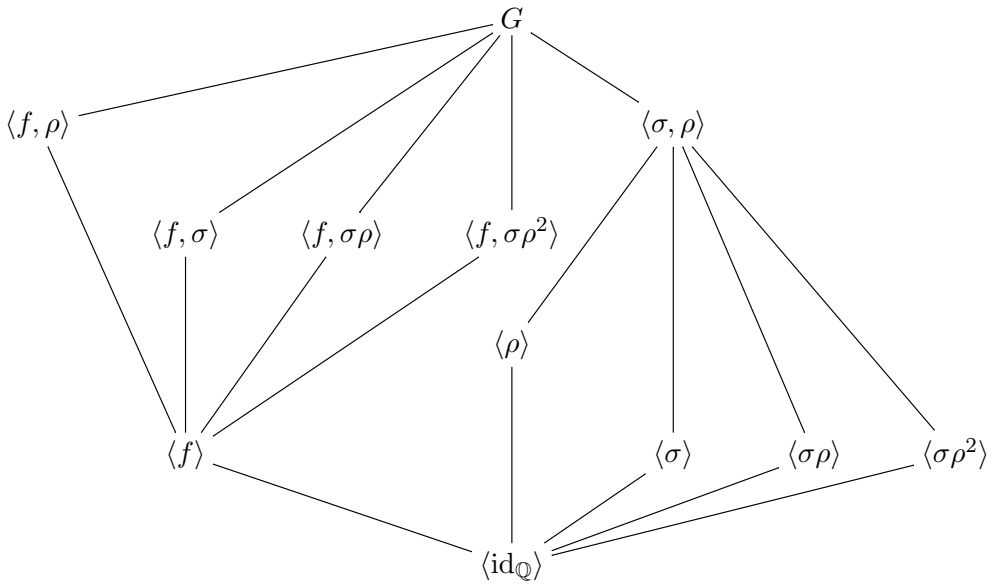
Решење. Корени датог полинома су $\pm\sqrt{2},\ \sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}$, где је $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ примитиван трећи корен из јединице. Према томе коренско поље је $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, i\sqrt{3})$.

Приметимо да је $|\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}| = 6$, што закључујемо посматрајући ланце $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ и $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ (из њих следи $2, 3 \mid |\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}| \leq 6$). Како је $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \leq \mathbb{R}$ имамо да је $|\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})| = 2$, па је $|K : \mathbb{Q}| = 12$.

Како је $|\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}| = 6$ (исти аргумент као и горе) закључујемо да $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ па је $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = \mathbb{Q}$. Јасно је да је $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = K$. Такође приметимо да су поља $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ Галоаова над $\mathbb{Q}$ јер су коренска поља редом полинома X^2-2 и X^3-2 над $\mathbb{Q}$. Према томе:

$$G = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{D}_3.^1$$

Ако је $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\mathrm{id}_\mathbb{Q}, f\}$ (где $f : \sqrt{2} \mapsto -\sqrt{2}$) и $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q}) = \{\mathrm{id}_\mathbb{Q}, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$ (ове аутоморфизме ћемо касније одредити), тада се лако може израчунати да је дијаграм подгрупа од G:



У следећој табели су дате информације о елементима $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})/\mathbb{Q})$:

$\sqrt[3]{2}$	$i\sqrt{3}$	ε	ред	ознака
$\sqrt[3]{2}$	$i\sqrt{3}$	ε	1	$\mathrm{id}_\mathbb{Q}$
$\sqrt[3]{2}$	$-i\sqrt{3}$	ε^2	2	σ
$\varepsilon\sqrt[3]{2}$	$i\sqrt{3}$	ε	3	ρ
$\varepsilon\sqrt[3]{2}$	$-i\sqrt{3}$	ε^2	2	$\sigma\rho^2$
$\varepsilon^2\sqrt[3]{2}$	$i\sqrt{3}$	ε	3	ρ^2
$\varepsilon^2\sqrt[3]{2}$	$-i\sqrt{3}$	ε^2	2	$\sigma\rho$

Стандардним рачуном фиксних поља добијамо следеће резултате.

Фиксна поља подгрупа реда 2 су: $K^{\langle f\rangle} = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$, $K^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, $K^{\langle\sigma\rho\rangle} = \mathbb{Q}(\sqrt{2}, \varepsilon\sqrt[3]{2})$ и $K^{\langle\sigma\rho^2\rangle} = \mathbb{Q}(\sqrt{2}, \varepsilon^2\sqrt[3]{2})$.

Фиксно поље подгрупе реда 3 је: $K^{\langle\rho\rangle} = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$.

Фиксна поља подгрупа реда 4 су: $K^{\langle f,\sigma\rangle} = \mathbb{Q}(\sqrt[3]{2})$, $K^{\langle f,\sigma\rho\rangle} = \mathbb{Q}(\varepsilon\sqrt[3]{2})$ и $K^{\langle f,\sigma\rho^2\rangle} = \mathbb{Q}(\varepsilon^2\sqrt[3]{2})$.

Коначно, фиксна поља подгрупа реда 6 су: $K^{\langle f,\rho\rangle} = \mathbb{Q}(i\sqrt{3})$ и $K^{\langle\sigma,\rho\rangle} = \mathbb{Q}(\sqrt{2})$. ⊣

[1] $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ и $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})) \cong \mathbb{D}_3$ су познате ствари.

2. Испитати да ли постоји конструктибилан једнакокраки троугао површине 2 и обима 8.

Решење. Нека је a дужина крака, а $2b$ дужина основице једнакокраког троугла обима 8 и површине 2. Тада је $2a+2b=8$, тј. $a+b=4$ и $\frac{1}{2}b\sqrt{a^2-b^2}=2$. Одавде је $16=b^2((4-b)^2-b^2)=b^2(16-8b)=-8b^3+16b^2$, тј. b задовољава полином $8X^3-16X^2+16$, тј. полином X^3-2X^2+2. Овај полином је несводљив над $\mathbb{Q}$ (кандидати за корен су ±1 и ±2), па је $|\mathbb{Q}(b):\mathbb{Q}|=3$. Према томе b није конструктибилан, па не може да буде ни дати троугао. ⊣

3. Израчунати Галоаову групу полинома $p(X)=X^4+3X^3-3X-2$ над $\mathbb{Q}$.

Решење. Факторизацијом модуло 2 добијамо растав $p_2(X)=X^4+X^3+X=X(X^3+X^2+1)$. Факторизацијом модуло 5 добијамо несводљив полином $p_5(X)=X^4+3X^3+2X+3$. (Проверите!)

Како је $p_5(X)$ несводљив над $\mathbb{F}_5$, то је и $p(X)$ несводљив над $\mathbb{Z}$, па и над $\mathbb{Q}$. Према томе $p(X)$ је сепарабилан. Нека је $G=\mathrm{Gal}(p/\mathbb{Q})\leq\mathbb{S}_4$. Користећи Дедекиндови теорему на $p_2(X)$ и $p_5(X)$ добијамо да G садржи 3-цикл и 4-цикл. Они генеришу подгрупе H и K реда 3 и 4. Како је $H\cap K$ тривијалан, подскуп HK од G садржи 12 елемената. Дакле, $|G|\geq12$ и $|G|\mid|\mathbb{S}_4|=24$. Према томе, могуће је да $|G|=12$ и $|G|=24$. Једина подгрупа од $\mathbb{S}_4$ реда 12 је $\mathbb{A}_4$, али G не може бити $\mathbb{A}_4$ јер садржи 4-цикл. Према томе $|G|=24$, тј. $G=\mathbb{S}_4$. ⊣

4. Нека је k поље, $\mathrm{char}(k)=p>0$ и $\alpha\in k^a$. Доказати да је α сепарабилан акко $|k(\alpha):k|=|k(\alpha^p):k|$.

Решење. $\Rightarrow$: Јасно је да $k\leq k(\alpha^p)\leq k(\alpha)$, јер $\alpha^p\in k(\alpha)$. Како α задовољава полином $X^p-\alpha^p\in k(\alpha^p)[X]$, то $\mu_{\alpha,k(\alpha^p)}(X)\mid X^p-\alpha^p=(X-\alpha)^p$, али такође $\mu_{\alpha,k(\alpha^p)}(X)\mid\mu_{\alpha,k}(X)$. Дакле, $\mu_{\alpha,k(\alpha^p)}(X)\mid\mathrm{НЗД}((X-\alpha)^p,\mu_{\alpha,k}(X))$, па како је $\mu_{\alpha,k}(X)$ сепарабилан добијамо да је $\mathrm{НЗД}((X-\alpha)^p,\mu_{\alpha,k}(X))=X-\alpha$ и $\mu_{\alpha,k(\alpha^p)}(X)=X-\alpha$. Према томе $\alpha\in k(\alpha^p)$, одакле $k(\alpha)=k(\alpha^p)$.

$\Leftarrow$: Ако α није сепарабилан, тада је $\mu_{\alpha,k}(X)=q(X^p)$, за неки полином $q(X)\in k[X]$. Како је $q(X)$ несводљив (јер је $\mu_{\alpha,k}(X)$ несводљив) и $q(\alpha^p)=\mu_{\alpha,k}(\alpha)=0$ закључујемо да је $\mu_{\alpha^p,k}(X)=q(X)$. Тада је $|k(\alpha):k|=\deg\mu_{\alpha,k}(X)=p\cdot\deg\mu_{\alpha^p,k}(X)=p\cdot|k(\alpha^p):k|>|k(\alpha^p):k|$. ⊣

5. **(а)** Нека је D домен са јединственом факторизцијом и $P=\langle t\rangle\neq0$ прави прост идеал. Доказати да не постоји прост идеал Q такав да $0\subsetneq Q\subsetneq P$.

(б) Нека је k алгебарски затворено поље и $V=Z(f)$ нерастављива хиперповрш у $\mathbb{A}_k^n$. Доказати да не постоји нерастављив алгебарски скуп W такав да $V\subsetneq W\subsetneq\mathbb{A}_k^n$.

Решење. **(а)** Претпоставимо да је Q прост идеал такав да $0\subsetneq Q\subsetneq P$. Како је Q прост и D домен са јединственом факторизацијом, то Q садржи несводљив елемент a.[2] Како $a\in P$, запишимо $a=bt$. Тада $bt\in Q$, $t\notin Q$ и Q прост повлаче $b\in Q$. Из $a=bt$, a несводљив и $t\notin D^\times$ јер је P прави идеал, добијамо $b\in D^\times$. Одатле је $Q=D$. Контрадикција.

(б) Нерастављиви алгебарски скупови у $\mathbb{A}_k^n$ су у 1-1 и на коресподенцији $W\mapsto I(W)$ са простим идеалима у $k[X_1,X_2,\ldots,X_n]$ (који је домен са јединственом факторизацијом). $I(\mathbb{A}_k^n)=0$ и $I(V)=I(Z(f))=\langle f\rangle$, јер је $Z(f)$ нерастављив. Дакле, тврђење следи из **(а).** ⊣

[2] Нека је $x\in Q$ ненула елемент и $x=q_1q_2\ldots q_k$ његова факторизација у несводљиве. Како је Q прост, тада бар један од q_i, $1\leq i\leq k$ припада Q.