Алгебра 3, Јул 2013. *21. јун 2013.*

А Претпоставимо да је $|\mathbb{Q}(\alpha):\mathbb{Q}|=8$. Ако је $\mathbb{Q}(\alpha)\mid\mathbb{Q}$ Галоаово раширење, доказати да је α конструктибилан. Испитати да ли важи обратно.

Решење. Докажимо најпре: ако је G група реда 2^n, тада постоји низ подгрупа $\langle e\rangle = H_0 < H_1 < \ldots < H_n = G$ такав да $|H_{i+1}:H_i|=2$, $0\le i<n$. Доказујемо индукциојом по n. За $n=1$ тврђење је очигледно. Претпоставимо да тврђење важи за групе реда 2^{n-1}. Нека је $|G|=2^n$. Знамо да G има нетривијалан центар, па по Кошијевој леми изаберимо у центру елемент a реда 2. Тада је $\langle a\rangle \triangleleft G$. По индуктивној хипотези у групи $G/\langle a\rangle$ постоји низ подгрупа $\langle\langle a\rangle\rangle = H_0 < H_1 < \ldots < H_{n-1} = G/\langle a\rangle$. Ако са π означимо канонски епиморфизам $G\longrightarrow G/\langle a\rangle$, тада је $\langle e\rangle < \langle a\rangle = \pi^{-1}[H_0] < \pi^{-1}[H_1] < \ldots < \pi^{-1}[H_{n-1}] = G$ тражени низ.

Претпоставимо сада да је раширење $\mathbb{Q}(\alpha)\mid\mathbb{Q}$ Галоаово степена 2^n. Изаберимо низ подгрупа $\langle \mathrm{id}\rangle = H_0 < H_1 < \ldots < H_n = \mathrm{gal}(\mathbb{Q}(\alpha)\mid\mathbb{Q})$ тако да је $|H_{i+1}:H_i|=2$. По теореми о коресподенцији тада имамо низ међупоља: $\mathbb{Q}(\alpha)=F_0>F_1>\ldots>F_n=\mathbb{Q}$ и $|F_i:F_{i+1}|=2$. То значи да је α конструктибилан број.

Обратно не важи. Приметимо да је $\sqrt[2^n]{2}$ очигледно конструктибилан број, али $\mathbb{Q}(\sqrt[2^n]{2})\mid\mathbb{Q}$ није нормално раширење за $n\ge 2$ (зато што му не припада 2^n-ти примитиван корен из јединице).

Б Дат је полином $f(x)=x^6-4\in\mathbb{Q}[x]$. Одредити коренско поље K полинома $f(x)$, описати елементе групе $\mathrm{gal}(K\mid\mathbb{Q})$ и одредити потпуну Галоаову коресподенцију тог раширења.

Решење. Означимо са $\varepsilon = e^{\frac{2pi}{6}} = \frac{1}{2}+\frac{i\sqrt{3}}{2}$. Тада су корени полинома $f(x)$: $\varepsilon^i\sqrt[3]{2}$, $0\le i<6$. Дакле, коренско поље $K=\mathbb{Q}(\sqrt[3]{2},\varepsilon)=\mathbb{Q}(\sqrt[3]{2},i\sqrt{3})$ и стандардно видимо да је $|K:\mathbb{Q}|=6$. Према томе сви елементи $\mathrm{gal}(K\mid\mathbb{Q})$ су описани (стандардним закључивањем) у следећој таблици (приметите да је ε^2 примитивни трећи корен из јединице). У таблици су израчунати и редови елемената из којих се види да је $\mathrm{gal}(K\mid\mathbb{Q})\cong\mathbb{D}_3$, као и како један изоморфизам изгледа:

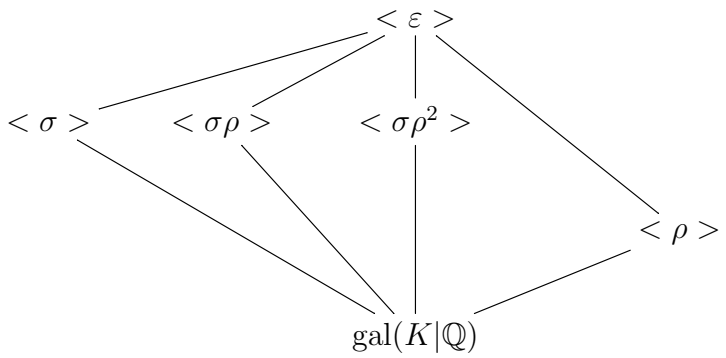
	$\sqrt[3]{2}$	$i\sqrt{3}$	ε	ред	изо.
f_1	$\sqrt[3]{2}$	$i\sqrt{3}$	ε	1	ε
f_2	$\sqrt[3]{2}$	$-i\sqrt{3}$	ε^5	2	σ
f_3	$\varepsilon^2\sqrt[3]{2}$	$i\sqrt{3}$	ε	3	ρ
f_4	$\varepsilon^2\sqrt[3]{2}$	$-i\sqrt{3}$	ε^5	2	$\sigma\rho^2$
f_5	$\varepsilon^4\sqrt[3]{2}$	$i\sqrt{3}$	ε	3	ρ^2
f_6	$\varepsilon^4\sqrt[3]{2}$	$-i\sqrt{3}$	ε^5	2	$\sigma\rho$

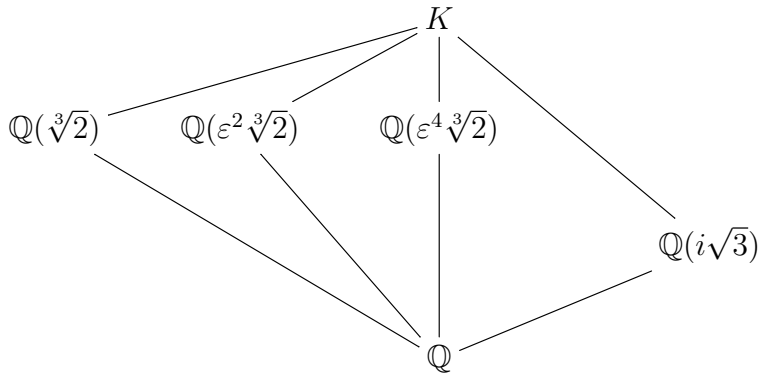
Нетривијалне подгрупе од $\mathbb{D}_3$ су: $\langle\rho\rangle$, $\langle\sigma\rangle$, $\langle\sigma\rho\rangle$ и $\langle\sigma\rho^2\rangle$. Одредимо њихова фиксна поља.

Видимо да је $\sigma(\sqrt[3]{2})=\sqrt[3]{2}$, одакле $\mathbb{Q}(\sqrt[3]{2})\le K^{<\sigma>}$. Но како је $|K^{<\sigma>}:\mathbb{Q}| = |\mathrm{gal}(K|\mathbb{Q}) :< \sigma > | = 3$ и како је $|\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}|=3$, из ланчаног правила добијамо $|K^{<\sigma>}:\mathbb{Q}(\sqrt[3]{2})|=1$, тј. $K^{<\sigma>}=\mathbb{Q}(\sqrt[3]{2})$.

Слично, ако уочимо да је $\sigma\rho(\varepsilon^2\sqrt[3]{2}) = \varepsilon^{10}\varepsilon^4\sqrt[3]{2} = \varepsilon^2\sqrt[3]{2}$, добићемо да је $K^{\langle\sigma\rho\rangle}=\mathbb{Q}(\varepsilon^2\sqrt[3]{2})$. И слично, $K^{\langle\sigma\rho^2\rangle}=\mathbb{Q}(\varepsilon^4\sqrt[3]{2})$. Коначно, на исти начин закључујемо да је $K^{\langle\rho\rangle}=\mathbb{Q}(i\sqrt{3})$.

Коресподенција се види на дијаграмима:





В За које просте бројеве p је једначина $x^p - p^p x + p = 0$ решива у радикалима? Одговор детаљно образложити.

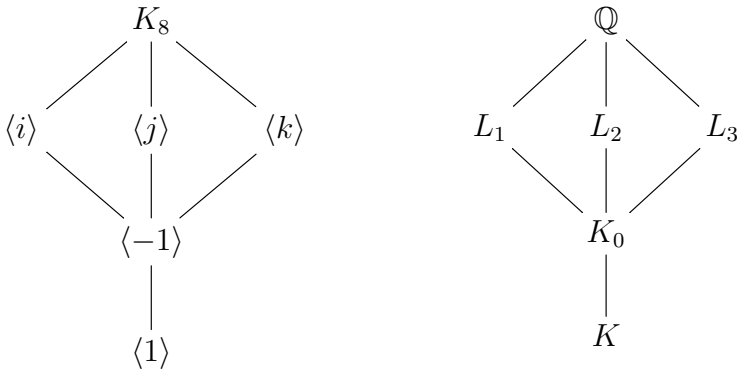
Решење. Означимо $f(x) = x^p - p^p x + p$. За $p = 2$ и $p = 3$ знамо да је $f(x) = 0$ решива у радикалима. Доказаћемо да за просте бројеве $p \geq 5$ то није тачно.

Одредимо најпре колико $f(x)$ има реалних нула. $f'(x) = px^{p-1} - p^p$, па нуле првог извиода задовољавају $x^{p-1} = p^{p-1}$, одакле закључујемо да имамо само две реалне нуле (јер је $p - 1$ паран број): $-p$ и p. Дакле, $f(x)$ има два локална екстремума. Приметимо да је $\lim_{x \longleftarrow -\infty} f(x) = -\infty$, $\lim_{x \longrightarrow \infty} f(x) = \infty$, па $f(x)$ у $-p$ има локални максимум, а у p локални минимум. Такође, како је $f(-p) = -p^p + p^p p + p = (p-1)p^p + p > 0$ и $f(p) = p^p - p^p p + p = (1-p)p^p + p < 0$, то закључујемо да $f(x)$ има три реалне нуле, и $(p-3)/2$ пара коњуковано комплексних нула.

Приметимо да је по Ајзенштајновом критеријуму $f(x)$ несводљив полином, па се $\mathrm{gal}(f \mid \mathbb{Q})$ утапа у $\mathbb{S}_p$. Такође, како је $f(x)$ минимални полином за сваки свој корен, можемо закључити да постоји елемент реда p у групи $\mathrm{gal}(f \mid \mathbb{Q})$; посматрајући га као елемент од $\mathbb{S}_p$ закључујемо да је у питању $p-$цикл. Одавде следи да је $\mathrm{gal}(f \mid \mathbb{Q})$ транзитивна подгрупа од $\mathbb{S}_p$. Такође, рестрикција коњуговања на коренско поље од f над $\mathbb{Q}$ је један елемент од $\mathrm{gal}(f \mid \mathbb{Q})$ који како смо видели има тачно 3 фиксне тачке. Према томе $\mathrm{gal}(f \mid \mathbb{Q})$ је транзитивна подгрупа од $\mathbb{S}_p$ која садржи пермутацију са тачно три фиксне тачке, па према задатку са вежби она није решива. Следи да $f(x) = 0$ није решива у радикалима.

Г Претпоставимо да је $K \mid \mathbb{Q}$ Галоаово раширење и претпоставимо да је $\mathrm{gal}(K \mid \mathbb{Q})$ група кватерниона. Ако је $L < K$ такво да $|L : \mathbb{Q}| = 2$, доказати да је $L \leq \mathbb{R}$.

Решење. Уочимо дијаграм подгрупа групе кватерниона и по теореми о коресподенцији одговарајући дијаграм међуполја:



Са дијаграма је јасно да је довољно доказати да је $K_0 \leq \mathbb{R}$, јер K_0 садржи сва квадратична раширења поља $\mathbb{Q}$ у K. Ако је $K \leq \mathbb{R}$ ствар је јасна. Претпоставимо да $K \not\leq \mathbb{R}$. Означимо са $K' = K \cap \mathbb{R}$. Доказаћемо $K' = K_0$, што завршава посао. Приметимо да је $K = \mathbb{Q}(\alpha)$ за неко $\alpha \in \mathbb{C} - \mathbb{R}$, што следи из теореме о примитивном елементу. Тада је и $K = K'(\alpha)$. Како је $K \mid \mathbb{Q}$ нормално, и како је и $\overline{\alpha}$ сигурно корен минималног полинома за α над $\mathbb{Q}$, закључујемо да $\overline{\alpha} \in K$. Тада и $\alpha + \overline{\alpha} \in K \cap \mathbb{R} = K'$. Дакле, како $\alpha + \overline{\alpha} \in K'$, то $K'(\alpha - \overline{\alpha}) = K'(\alpha) = K$, тј. $K = K'(i\beta)$, где је β реалан. Како $(i\beta)^2 = -\beta^2 \in K \cap \mathbb{R} = K'$, и како $i\beta \notin K'$, то је $|K : K'| = 2$, одакле закључујемо што смо желели: $K' = K_0$.

Д Нека је $\Phi_n(x)$ $n-$ти циклотомични полином, и нека је p непаран прост број такав да $p \nmid n$. Претпоставимо да за неко $a \in \mathbb{Z}$ важи $p \mid \Phi_n(a)$.

1° Доказати да је ред од a модуло p једнак n.

2° Доказати да $n \mid p-1$.

3° Доказати да постоји бесконачно много простих бројева p таквих да $n \mid p-1$.

Решење. Сетимо се са вежби да је $x^n - 1 = \prod_{d|n} \Phi_d(x) = \phi_n(x) \prod_{d|n,\, d<n} \Phi_d(x)$. Ако $p \mid \Phi_n(a)$, тада $a^n =_p 1$. Означимо са m ред елемента a модуло p; тада $m \mid n$. Ако претпоставимо да је $m < n$ тада из $x^m - 1 = \prod_{d|m} \Phi_d(x)$ закључујемо да $p \mid \Phi_d(a)$, где $d \mid m$, па и $d \mid n$. (Ако се мало удубимо, закључићемо заправо да $p \mid \Phi_m(a)$.) Како $d \mid n$ и $d < n$, ако се вратимо да је $x^n - 1 = \phi_n(x) \prod_{d|n,\, d<n} \Phi_d(x)$, добијамо да је a двострука нула полинома $x^n - 1$ модуло p. Међутим то је контрадикција, јер из претпоставке $p \nmid n$ имамо да је $x^n - 1$ сепарабилан модуло p. Дакле, заиста је a реда n модуло p.

Специјално, $(a, p) = 1$, па по малој Фермаовој теореми је $a^{p-1} =_p 1$, одакле директно закључујемо да $n \mid p-1$.

Лема. Ако је $f(x)$ моничан полинома са целобројним коефицијентима, тада постоји бесконачно много простих бројева који деле бројеве $f(1), f(2), f(3), \ldots$

Трећи део задатка директно следи из леме и претходно доказаног: према леми постоји бесконачно много простих бројева који деле $\Phi_n(1), \Phi_n(2), \Phi_n(3), \ldots$, а само коначно много од њих може да дели n. За бесконачно много преосталих p важи да $p \nmid n$ и $p \mid \Phi_n(a)$, за неко a, па $n \mid p-1$.

Доказ леме. Претпоставимо супротно да само прости бројеви $p_1, \ldots, p_k$ деле $f(1), f(2), f(3), \ldots$ Означимо са $P = p_1 p_2 \ldots p_k$. Изаберимо n такав да је $f(n) = a \neq 0$. Посматрајмо полином $f(n + aPx)$. Ако је $f(x) = \sum_{i=0}^{m} a_i x^i$, где је $a_m = 1$, тада је:

$$\begin{aligned}
f(n+aPx) &= \sum_{i=0}^{m} a_i (n+aPx)^i \\
&= \sum_{i=0}^{m} a_i \sum_{j=0}^{i} \binom{i}{j} n^{i-j} a^j P^j x^j \\
&= \sum_{i=0}^{m} \left[a_i n^i + a_i \sum_{j=1}^{i} \binom{i}{j} n^{j-i} a^j P^j x^j \right] \\
&= \sum_{i=0}^{m} a_i n^i + \sum_{i=1}^{m} a_i \sum_{j=1}^{i} \binom{i}{j} n^{j-i} a^j P^j x^j \\
&= f(n) + aP \sum_{i=1}^{m} a_i \sum_{j=1}^{i} \binom{i}{j} n^{j-i} a^{j-1} P^{j-1} x^j \\
&= a + aP \sum_{i=1}^{m} a_i \sum_{j=1}^{i} \binom{i}{j} n^{j-i} a^{j-1} P^{j-1} x^j.
\end{aligned}$$

Одавде видимо да је $f(n + aPx) = ag(x)$, где је полином

$$g(x) = 1 + P \sum_{i=1}^{m} a_i \sum_{j=1}^{i} \binom{i}{j} n^{j-i} a^{j-1} P^{j-1} x^j$$

са целобројним коефицијентима. Сада такође видимо да је $g(x) =_P 1$, за све $x = 1, 2, 3, \ldots$ Изаберимо n_0 и прост број p различит од $p_1, p_2, \ldots, p_k$ такав да $p \mid g(n_0)$. Тада $p \mid ag(n_0) = f(n + aPn_0)$, што је контрадикција.