MATH 4EE3 - Assignment 2

Greg Baril
Geoff Williams
Paul Vrbik

Brought to you by the [GEOFF] Williams school of awesome

April 5, 2006

Question 12.3 Let $\gamma = \sqrt{2+\sqrt{2}}$. Show that $\mathbb{Q}(\gamma):\mathbb{Q}$ is normal, with cyclic Galois group. Show that $\mathbb{Q}(\gamma, i) = \mathbb{Q}(\sigma)$ where $\sigma^4 = i$.

Let $\gamma = \sqrt{2+\sqrt{2}}$ where we have that $\gamma^4 - 4\gamma^2 + 2 = 0 \Rightarrow \gamma$ is a root of $f(x) = x^4 - 4x^2 + 2$ which is irreducible by Eisenstein. It is also the case that $f(-\gamma) = f(\beta) = f(-\beta) = 0$ where $\beta = \sqrt{2-\sqrt{2}}$.

Trivially $\gamma, -\gamma \in \mathbb{Q}(\gamma)$ and since $\sqrt{2} = \sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}}$ where $\sqrt{2} = \gamma^2 - 2 \in \mathbb{Q}(\gamma)$ we have that $\beta = \sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in \mathbb{Q}(\gamma)$.

Since all the roots of f are in $\mathbb{Q}(\gamma)$ we may conclude that $\mathbb{Q}(\gamma)$ is a splitting field for $f(x)$ over the fixed field $\mathbb{Q}$ such that it is normal over $\mathbb{Q}$.

This implies that, since the extension is normal that $[\mathbb{Q}(\gamma):\mathbb{Q}] = |Gal(\mathbb{Q}(\gamma)/\mathbb{Q})| = 4$

We have the any automorphism $\sigma \in Gal(\mathbb{Q}(\gamma)/\mathbb{Q})$ satisfies:

$$\sigma^2\left(\sqrt{2+\sqrt{2}}\right) = \sigma\left(\sqrt{2-\sqrt{2}}\right) = \frac{\sigma(\gamma^2-2)}{\sigma(\gamma)} = \frac{\beta^2-2}{\beta} = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\sqrt{2+\sqrt{2}}$$

$$\sigma^3\left(\sqrt{2+\sqrt{2}}\right) = \frac{\sigma\left(-\sqrt{2}\right)}{\sigma\left(\sqrt{2+\sqrt{2}})\right)} = \frac{\frac{\sqrt{2}}{-\sqrt{2}}}{\sqrt{2-\sqrt{2}}} = -\sqrt{2-\sqrt{2}}$$

$$\sigma^4\left(\sqrt{2+\sqrt{2}}\right) = \sigma\left(-\sqrt{2-\sqrt{2}}\right) = \sqrt{2+\sqrt{2}}$$

Since $\sigma^4(\gamma) = \gamma$ we have that γ is an element of order 4 which would imply that $Gal(\mathbb{Q}(\gamma)/\mathbb{Q})$ is cyclic. Where:

$$[\mathbb{Q}(\gamma, i):\mathbb{Q}(\gamma)] = 2$$
$$[\mathbb{Q}(\gamma):\mathbb{Q}] = 4$$
$$[\mathbb{Q}(\gamma, i):\mathbb{Q}] = 2$$

Now take $\phi^4 = i$ then $\phi^8 = -1$ so ϕ is a zero of $f(x) = x^8 + 1$ and $[\mathbb{Q}(\phi):\mathbb{Q}] = 8$.

Since $\mathbb{Q} \subset \mathbb{Q}(\phi)(\gamma, i)$ when the extensions have the same degree we have that $\mathbb{Q}(\phi) = \mathbb{Q}(\phi, i)$.

Consdier $\gamma + \beta i \in \mathbb{Q}(\gamma, i)$

$$\begin{aligned}(\gamma+\beta i)^4 &= \gamma^4 + 4\gamma^3\beta i - 6\gamma^2\beta^2 - 4\gamma\beta^3 i + \beta^4 \\ &= 4\sqrt{2}i(2+\sqrt{2}-2+\sqrt{2}) \\ &= 16i\end{aligned}$$

Therefore $\phi \in \mathbb{Q}(\gamma, i)$ so $\mathbb{Q}(\phi) \subset \mathbb{Q}(\gamma, i)$ and so $\mathbb{Q}(\phi) = \mathbb{Q}(\gamma, i)$.

Question 12.4 Find the Galois group of $t^6 - 7$ over $\mathbb{Q}$

By Eisenstein $t^6 - 7$ is irreducible over $\mathbb{Q}$.
Since $t = \pm\sqrt[6]{7}$ we let:

$$\alpha \in \{\sqrt[6]{7}, \zeta_3\alpha, \zeta_3^2\alpha\}$$
$$\beta \in \{-\sqrt[6]{7}, \zeta_3\beta, \zeta_3^2\beta\}$$

We know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ (because α is not a root of the irreducible polynomial of degree 6) and that $[\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}(\alpha)] = 2$ which means that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 6 = 12$.
We create the twelve automorphisms σ_{ij} that follow the properties:

$$\sigma_{ij}(\alpha) \rightarrow x \in \{\alpha, \zeta_3\alpha, \zeta_3^2\alpha, \beta, \zeta_3\beta, \zeta_3^2\beta\}$$
$$\sigma_{ij}(\zeta_3) \rightarrow x \in \{\zeta_3, \zeta_3^2\}$$

We say σ_{11} is the automorphism that takes $\alpha \rightarrow \alpha$ and $\zeta_3 \rightarrow \zeta_3$, σ_{21} is the automorphism that takes $\alpha \rightarrow \zeta_3\alpha$ and $\zeta_3 \rightarrow \zeta_3$ and so on.
Investigating the order of each σ we find that:

$\lvert\zeta_{11}\rvert = 1$	$\lvert\zeta_{12}\rvert = 2$
$\lvert\zeta_{21}\rvert = 3$	$\lvert\zeta_{22}\rvert = 2$
$\lvert\zeta_{31}\rvert = 2$	$\lvert\zeta_{32}\rvert = 2$
$\lvert\zeta_{41}\rvert = 2$	$\lvert\zeta_{42}\rvert = 2$
$\lvert\zeta_{51}\rvert = 6$	$\lvert\zeta_{52}\rvert = 3$
$\lvert\zeta_{61}\rvert = 2$	$\lvert\zeta_{62}\rvert = 4$

Where the only group with elements of these orders is the dihedral group of order 4, D_4.

Question 13.1 (a) Find the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ because $\sqrt{2}$ has $m_a(x) = x^2 - 2$ over $\mathbb{Q}$ and $[\mathbb{Q}(\sqrt{5}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 2$ becuse $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$ and $\sqrt{5}$ has $m_a(x) = x^2 - 5$ over $\mathbb{Q}(\sqrt{2})$.

So our Galois group has order 4

$$\begin{array}{lll} \sigma\left(\sqrt(2)\right) \to \sqrt{2} & \sigma\left(\sqrt(5)\right) \to \sqrt{5} & |\sigma| = 1 \\ \sigma\left(\sqrt(2)\right) \to -\sqrt{2} & \sigma\left(\sqrt(5)\right) \to \sqrt{5} & |\sigma| = 2 \\ \sigma\left(\sqrt(2)\right) \to \sqrt{2} & \sigma\left(\sqrt(5)\right) \to -\sqrt{5} & |\sigma| = 2 \\ \sigma\left(\sqrt(2)\right) \to -\sqrt{2} & \sigma\left(\sqrt(5)\right) \to -\sqrt{5} & |\sigma| = 2 \end{array}$$

Where the only group with four elements satisfying these orders is $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Question 13.1 (b) Find the Galois group of $\mathbb{Q}(\alpha) : \mathbb{Q}$ where $\alpha = \exp(2\pi i/3)$

$\alpha = \zeta_3$ which is a solution to $x^3 - 1$. But we know 1 is a root of $x^3 - 1$ so the minimal polynomial becomes $m_a(x) = x^2 + x + 1$. So $m_a(x)$ has roots ζ_3 and ζ_3^2 over $\mathbb{Q}$.

So the Galois group has order 2 and the elements are $\sigma_1(\zeta_3) \to \zeta_3$ and $\sigma_2(\zeta_3) \to \zeta_3^2$. This is $\mathbb{Z}_2$.

Question 13.1 (c) Find the Galois group of $K : \mathbb{Q}$ where K is the splitting filed over $\mathbb{Q}$ for $t^4 - 3t^2 + 4$.

Let $x = t^2$ so we have $x^2 - 3x + 4$ and $x = \frac{3 \pm \sqrt{-7}}{2}$ which implies that

$$t = \frac{\pm\sqrt{3 \pm \sqrt{-7}}}{2}$$

so letting $\alpha = \frac{\sqrt{3+\sqrt{-7}}}{2}$, $\beta = \frac{\sqrt{3-\sqrt{-7}}}{2}$ where $\alpha \cdot \beta = 2$.

Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $\mathbb{Q}(\alpha)$ is a splitting field for our polynomial.

$$\begin{array}{ll} \sigma_1(\alpha) = \alpha & |\sigma| = 1 \\ \sigma_2(\alpha) = -\alpha & |\sigma| = 2 \\ \sigma_3(\alpha) = \beta & |\sigma| = 2 \\ \sigma_4(\alpha) = -\beta & |\sigma| = 4 \end{array}$$

Where the only group with four elements satisfying these orders is $\mathbb{Z}_4$.

Question 13.10 Find the Galois group of $t^8 + t^4 + 1$ over $\mathbb{Q}(i)$.

We have that

$$t^8 + t^4 + 1 = (t^4 - t^2 + 1)(t^2 + t + 1)(t^2 - t + 1)$$

where $t^2 + t + 1$ has roots $\frac{-1 \pm i\sqrt{3}}{2}$, $t^2 - t + 1$ has roots $\frac{1 \pm i\sqrt{3}}{2}$, and $t^4 - t^2 + 1$ has roots $\sqrt{\frac{1 \pm i\sqrt{3}}{2}}$.

The roots of t^2+t+1 and t^2-t+1 can be found from $\sqrt{\frac{1+i\sqrt{3}}{2}}$. Also $\frac{1 \pm i\sqrt{3}}{2}$ are roots of unity equal to $\exp(\frac{2\pi i}{3})$ and $\exp(\frac{4\pi i}{3})$. The square roots of these are $\exp(\frac{\pi i}{3})$ and $\exp(\frac{2\pi i}{3})$. Thus $\frac{\sqrt{1-i\sqrt{3}}}{2}$ can be formed from $\frac{\sqrt{1+i\sqrt{3}}}{2}$ which shows that the splitting field is $\mathbb{Q}\left(\sqrt{\frac{1+i\sqrt{3}}{2}}\right)$ and $\mathbb{Q}\left(\sqrt{\frac{1+i\sqrt{3}}{2}}\right) : \ntrianglerighteq] = 4$ because $m_a(t) = t^4 - t^2 + 1$. Our four automorphisms have the following form:

$$\sigma_1\left(\frac{\sqrt{1+i\sqrt{3}}}{2}\right) = \frac{\sqrt{1+i\sqrt{3}}}{2} \qquad |\sigma_1| = 1$$

$$\sigma_2\left(\frac{\sqrt{1+i\sqrt{3}}}{2}\right) = -\frac{\sqrt{1+i\sqrt{3}}}{2} \qquad |\sigma_2| = 2$$

$$\sigma_3\left(\frac{\sqrt{1+i\sqrt{3}}}{2}\right) = \frac{\sqrt{1-i\sqrt{3}}}{2} \qquad |\sigma_3| = 2$$

$$\sigma_4\left(\frac{\sqrt{1+i\sqrt{3}}}{2}\right) = -\frac{\sqrt{1-i\sqrt{3}}}{2} \qquad |\sigma_4| = 2$$

Where the only group with four elements satisfying these orders is $\mathbb{Z}_2 \times \mathbb{Z}_2$.