Math 503: Abstract Algebra
Homework 10

Lawrence Tyler Rush
<me@tylerlogic.com>

April 18, 2014
http://coursework.tylerlogic.com/courses/upenn/math503/homework10

1 Determine the Galois group of the splitting field of $T^4 - 3$

Since the polynomial $T^4 - 3$ can be broken down via the difference of squares as

$$T^4 - 3 = (T^2 - \sqrt{3})(T^2 + \sqrt{3}) = (T^2 - \sqrt{3})(T^2 - (-\sqrt{3})) = (T - \sqrt[4]{3})(T + \sqrt[4]{3})(T - i\sqrt[4]{3})(T + i\sqrt[4]{3})$$

then the roots are $\pm\sqrt[4]{3}, \pm i\sqrt[4]{3}$. So the splitting field of $T^4 - 3$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$. This yields

$$\left\{ \begin{array}{lll} \sqrt[4]{3} & \mapsto & \pm\sqrt[4]{3} \\ i\sqrt[4]{3} & \mapsto & \pm i\sqrt[4]{3} \end{array} \right. \qquad \left\{ \begin{array}{lll} \sqrt[4]{3} & \mapsto & \pm i\sqrt[4]{3} \\ i\sqrt[4]{3} & \mapsto & \pm\sqrt[4]{3} \end{array} \right. \tag{1.1}$$

as the possible elements of the Galois group of K, leaving us with a potential Galois group of size 8.

Now since $T^4 - 3$ is irreducible over $\mathbb{Q}$ (by Eisenstein's criteria), then $\mathbb{Q}(\sqrt[4]{3})$ is an extension of degree four. In $\mathbb{Q}(\sqrt[4]{3})$, $T^4 - 3$ factors as $T^4 - 3 = (T - \sqrt[4]{3})(T + \sqrt[4]{3})(T^2 + \sqrt{3})$ where $(T^2 + \sqrt{3})$ is irreducible with roots $\pm i\sqrt[4]{3}$. Then $K = \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$ is an extension of degree two over $\mathbb{Q}(\sqrt[4]{3})$. Therefore K has degree 8 over $\mathbb{Q}$, and this implies that the 8 automorphisms above are all elements of the Galois group of K, and furthermore are the only elements.

Note that every automorphism σ of the Galois group of K will take $\sqrt[4]{3}$ to an element in K of the form $(-1)^m i^n \sqrt[4]{3}$ and therefore take $i\sqrt[4]{3}$ to an element of the form $(-1)^r i^{n+1}\sqrt[4]{3}$ for $m, n, r \in \{0, 1\}$. This then defines the mapping of i as

$$\sigma(i) = \sigma^{-1}(\sqrt[4]{3})\sigma(i\sqrt[4]{3}) = ((-1)^m i^n \sqrt[4]{3})^{-1}(-1)^r i^{n+1}\sqrt[4]{3} = (-1)^{r-m} i$$

Conversly if we were to define the the mapping of only $\sqrt[4]{3}$ and i, mapping them to $(-1)^m i^n \sqrt[4]{3}$ and $(-1)^r i$, respectively, we can recover where $i\sqrt[4]{3}$ is mapped to as $(-1)^r i(-1)^m i^n \sqrt[4]{3} = (-1)^{r+m} i^{n+1}\sqrt[4]{3}$, resulting in one of the automorphisms in equation 1.1. Hence, we can simply define an automorphism in $\mathrm{Gal}(K/\mathbb{Q})$ by its mapping of $\sqrt[4]{3}$ to any other root of $T^4 - 3$ and its mapping of i to $\pm i$.

So let's define

$$\sigma = \left\{ \begin{array}{lll} \sqrt[4]{3} & \mapsto & i\sqrt[4]{3} \\ i & \mapsto & i \end{array} \right. \qquad \tau = \left\{ \begin{array}{lll} \sqrt[4]{3} & \mapsto & \sqrt[4]{3} \\ i & \mapsto & -i \end{array} \right.$$

form which we see $|\sigma| = 4$ and $|\tau| = 2$. Furthermore we see that σ and τ generate $\mathrm{Gal}(K/\mathbb{Q})$ since any automorphism

$$\left\{ \begin{array}{lll} \sqrt[4]{3} & \mapsto & i^m \sqrt[4]{3} \\ i & \mapsto & (-1)^n i \end{array} \right.$$

in the Galois group, where $m \in \{0, 1, 2, 3\}$ and $n \in \{0, 1\}$ is equal to $\sigma^m \tau^n$. Finally we have

$$\begin{array}{rcl} \tau\sigma^3(\sqrt[4]{3}) & = & \tau(-i\sqrt[4]{3}) = i\sqrt[4]{3} = \sigma(\sqrt[4]{3}) = \sigma\tau(\sqrt[4]{3}) \\ \tau\sigma^3(i) & = & \tau(i) = -i = \sigma(-i) = \sigma\tau(i) \end{array}$$

so that $\sigma\tau = \tau\sigma^3$. Since $|\sigma| = 4$ then this can be restated as $\sigma\tau = \tau\sigma$. Hence $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau | \sigma^4 = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$, or in other words, $\mathrm{Gal}(K/\mathbb{Q})$ is the dihedral group, D_8, of size eight.

2

(a)

(b)

(c) Extra Credit

3

(a)

Using the fact that $\zeta^2+\zeta+1=0$, $\alpha+\beta+\gamma=0$, $R(\zeta;\alpha,\beta,\gamma)=\alpha+\zeta\cdot\beta+\zeta^2\cdot\gamma$, and $R(\zeta^2;\alpha,\beta,\gamma)=\alpha+\zeta^2\cdot\beta+\zeta\cdot\gamma$, we have

$$\begin{aligned}
3\alpha &= 2\alpha-\beta-\gamma \\
&= 2\alpha+(\zeta^2+\zeta)\beta+(\zeta^2+\zeta)\gamma \\
&= \alpha+\zeta^2\beta+\zeta\beta+\alpha+\zeta^2\gamma+\zeta\gamma \\
&= (\alpha+\zeta\beta+\zeta^2\gamma)+(\alpha+\zeta^2\beta+\zeta\gamma) \\
&= R(\zeta;\alpha,\beta,\gamma)+R(\zeta^2;\alpha,\beta,\gamma)
\end{aligned}$$

Furthermore, since $\zeta^3=1$ then

$$\begin{aligned}
3\beta &= 2\beta-\alpha-\gamma \\
&= 2\beta+(\zeta^2+\zeta)\alpha+(\zeta^2+\zeta)\gamma \\
&= \beta+\zeta^2\alpha+\zeta\alpha+\beta+\zeta^2\gamma+\zeta\gamma \\
&= (\zeta^2\alpha+\beta+\zeta\gamma)+(\zeta\alpha+\beta+\zeta^2\gamma) \\
&= (\zeta^2\alpha+\zeta^3\beta+\zeta^4\gamma)+(\zeta\alpha+\zeta^3\beta+\zeta^2\gamma) \\
&= \zeta^2(\alpha+\zeta^1\beta+\zeta^2\gamma)+\zeta(\alpha+\zeta^2\beta+\zeta\gamma) \\
&= \zeta^2R(\zeta;\alpha,\beta,\gamma)+\zeta R(\zeta^2;\alpha,\beta,\gamma)
\end{aligned}$$

and finally

$$\begin{aligned}
3\gamma &= 2\gamma-\alpha-\beta \\
&= 2\gamma+(\zeta^2+\zeta)\alpha+(\zeta^2+\zeta)\beta \\
&= \gamma+\zeta^2\alpha+\zeta\alpha+\gamma+\zeta^2\beta+\zeta\beta \\
&= (\zeta\alpha+\zeta^2\beta+\gamma)+(\zeta^2\alpha+\zeta\beta+\gamma) \\
&= (\zeta\alpha+\zeta^2\beta+\zeta^3\gamma)+(\zeta^2\alpha+\zeta^4\beta+\zeta^3\gamma) \\
&= \zeta(\alpha+\zeta\beta+\zeta^2\gamma)+\zeta^2(\alpha+\zeta^2\beta+\zeta\gamma) \\
&= \zeta R(\zeta;\alpha,\beta,\gamma)+\zeta^2R(\zeta^2;\alpha,\beta,\gamma)
\end{aligned}$$

(b)

(c)

(d)

(e)

4 Extra Credit