MATH 3030, Abstract Algebra
Winter 2013
Toby Kenney
Homework Sheet 16
Model Solutions

Basic Questions

1. *Let f be an irreducible quartic (degree 4) polynomial over a perfect field F. Let K be a splitting field for f over F. Let the zeros of f in K be α, β, γ and δ.*

   (a) What is the orbit of $\alpha\beta + \gamma\delta$ under $G(K/F)$?

   $G(K/F)$ induces permutations on $\{\alpha, \beta, \gamma, \delta\}$. Under the symmetric group on this set, the orbit of $\alpha\beta + \gamma\delta$ is $\{\alpha\beta + \gamma\delta, \alpha\gamma + \beta\delta, \alpha\delta + \beta\gamma\}$.

   (b) [bonus] If $f(x) = x^4 + ax^3 + bx^2 + cx + d$, what is $\mathrm{Irr}(\alpha\beta + \gamma\delta, F)$?

   Since F is perfect, $\mathrm{Irr}(\theta, F)$ is the product $\Pi_{\theta'}(x - \theta')$ over all conjugate θ' of θ. In this case, this product is:

$$
\begin{aligned}
&(x - (\alpha\beta + \gamma\delta))(x - (\alpha\gamma + \beta\delta))(x - (\alpha\delta + \beta\gamma)) \\
&= x^3 - (\alpha\beta + \gamma\delta + \alpha\gamma + \beta\delta + \alpha\delta + \beta\gamma)x^2 \\
&+((\alpha\beta + \gamma\delta)(\alpha\gamma + \beta\delta) + (\alpha\beta + \gamma\delta)(\alpha\delta + \beta\gamma) + (\alpha\gamma + \beta\delta)(\alpha\delta + \beta\gamma))x \\
&-(\alpha\beta + \gamma\delta)(\alpha\gamma + \beta\delta)(\alpha\delta + \beta\gamma)
\end{aligned}
$$

   We need to evaluate the coefficients in terms of the elementary symmetric functions of α, β, γ and δ. The first is easy — $(\alpha\beta+\gamma\delta+\alpha\gamma+\beta\delta+\alpha\delta+\beta\gamma)$ is a elementary symmetric funtion — it is the coefficient b in the original polynomial.

   The other products are calculated as

$$
\begin{aligned}
&((\alpha\beta + \gamma\delta)(\alpha\gamma + \beta\delta) + (\alpha\beta + \gamma\delta)(\alpha\delta + \beta\gamma) + (\alpha\gamma + \beta\delta)(\alpha\delta + \beta\gamma)) \\
&= (\alpha + \beta + \gamma + \delta)(\alpha\beta\gamma + \alpha\beta\delta + \alpha\gamma\delta + \beta\gamma\delta) - 4\alpha\beta\gamma\delta \\
&= ac - 4d
\end{aligned}
$$

$$
\begin{aligned}
&(\alpha\beta + \gamma\delta)(\alpha\gamma + \beta\delta)(\alpha\delta + \beta\gamma) \\
&= \alpha\beta\gamma\delta(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) + (\alpha^2\beta^2\gamma^2 + \alpha^2\beta^2\delta^2 + \alpha^2\gamma^2\delta^2 + \beta^2\gamma^2\delta^2) \\
&= d(a^2 - 2b) + c^2 - 2db
\end{aligned}
$$

This gives that $\mathrm{Irr}(\alpha\beta+\gamma\delta, F) = x^3 - bx^2 + (ac-4d)x - (d(a^2-4b)+c^2)$.

2. *Write $\frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2}$ as a rational function in the elementary symmetric functions $a+b+c$, $ab+ac+bc$ and abc.*

   We see that $\frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2} = \frac{a^2b^2+b^2c^2+a^2c^2}{(abc)^2}$, so we just need to express $a^2b^2+b^2c^2+a^2c^2$ as a function of these elementary symmetric functions. We start by trying $(ab+bc+ac)^2$. This gives $a^2b^2+b^2c^2+a^2c^2+2(ab^2c+a^2bc+abc^2) = a^2b^2+b^2c^2+a^2c^2+2abc(a+b+c)$, so we deduce that

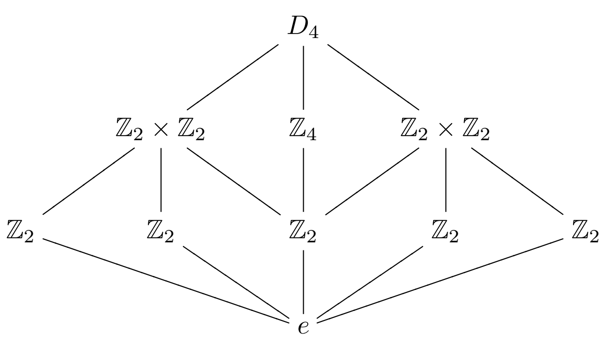
$$\frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2} = \frac{(ab+bc+ac)^2 - 2abc(a+b+c)}{(abc)^2}$$

3. *What is the order of $G(GF(64)/GF(4))$?*

   We know that GF(4) is perfect, so GF(64) is a separable extension, and a splitting field. Therefore, we know that $|G(GF(64)/GF(4))| = [GF(64) : GF(4)] = 3$.

4. *How many extension fields of $\mathbb{Q}$ are contained in the field $\mathbb{Q}(\sqrt[4]{3}, i)$?*

   $\mathbb{Q}(\sqrt[4]{3}, i)$ is the splitting field of $x^4 - 3$, so it is a normal extension of $\mathbb{Q}$. The zeros of x^4-3 are $\{\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}\}$. The automorphisms σ of $\mathbb{Q}(\sqrt[4]{3}, i)$ are entirely determined by $\sigma(\sqrt[4]{3})$ and $\sigma(i)$. There are 4 possibilities for $\sigma(\sqrt[4]{3}$ and 2 possibilities for $\sigma(i)$, so there are 8 automorphisms in total. This means that $G(\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q})$ is isomorphic to the dihedral group D_4. The subgroup lattice of D_4 looks like:



   The extension fields of $\mathbb{Q}$ contained in $\mathbb{Q}(\sqrt[4]{3}, i)$ correspond to the subgroups of D_4, so there are 10 in total (including $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{3}, i)$).

   [The extension fields are: $\mathbb{Q}$,$\mathbb{Q}(\sqrt{3})$,$\mathbb{Q}(i)$,$\mathbb{Q}(\sqrt{3}i)$,$\mathbb{Q}(\sqrt{3}, i)$,$\mathbb{Q}(\sqrt[4]{3})$,$\mathbb{Q}(\sqrt[4]{3}(1-i))$,$\mathbb{Q}(\sqrt[4]{3}(1+i))$,$\mathbb{Q}(\sqrt[4]{3}i)$ and $\mathbb{Q}(\sqrt[4]{3}, i)$.]

Theoretical Questions

5. *Let E be a finite normal extension of F. Let $\alpha \in E$. Define the* norm *of α over F by:*

$$N_{E/F}(\alpha) = \Pi_{\sigma \in G(E/F)} \sigma(\alpha)$$

and the trace *of α over F by:*

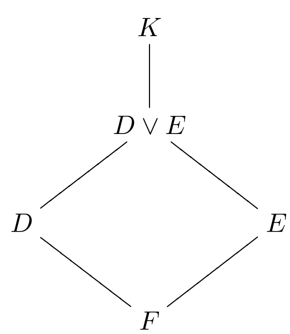
$$Tr_{E/F}(\alpha) = \sum_{\sigma \in G(E/F)} \sigma(\alpha)$$

Show that $N_{E/F}(\alpha)$ and $Tr_{E/F}(\alpha)$ are elements of F.

Let $\tau \in G(E/F)$, and consider $\tau(N_{E/F}(\alpha)) = \Pi_{\sigma \in G(E/F)} \tau\sigma(\alpha)$. Since left multiplication by τ gives a permutation on $G(E/F)$, we see that $\tau(N_{E/F}(\alpha)) = N_{E/F}(\alpha)$, that is, $N_{E/F}(\alpha)$ is in the fixed field of $G(E/F)$, which by the Galois correspondence is F. Therefore, we have shown that $N_{E/F}(\alpha) \in F$.

Similarly, for and $\tau \in G(E/F)$, $\tau(\mathrm{Tr}_{E/F}(\alpha)) = \sum_{\sigma \in G(E/F)} \tau\sigma(\alpha) = \mathrm{Tr}_{E/F}(\alpha)$, so $\mathrm{Tr}_{E/F}(\alpha)$ is in the fixed field of $G(E/F)$, so it is in F.

6. *Let D and E be two extension fields of F. Let K be an extension field of F containing both D and E. The join $D \vee E$ of D and E is the smallest subfield of K that contains both D and E as subfields — see the following diagram:*



Describe $G(K/(D \vee E))$ in terms of $G(K/D)$ and $G(K/E)$.

$G(K/D \vee E) = G(K/D) \cap G(K/E)$. To see this, we see that any $\sigma \in G(K/D) \cap G(K/E)$ must fix D and E, and since the set of fixed elements is a field, it must fix the smallest subfield containing both D and E, which is $D \vee E$. This shows that $G(K/D) \cap G(K/E) \subseteq G(K/D \vee E)$. On the other hand, if $\sigma \in G(K/(D \vee E))$, then it fixes $D \vee E$, so it fixes all subfields of $D \vee E$, which includes D and E. Therefore, we have $\sigma \in G(K/D)$ and $\sigma \in G(K/E)$, so we have shown $G(K/D \vee E) \subseteq G(K/D) \cap G(K/E)$.

7. *Let f be an irreducible monic polynomial over a field F, and let K be a splitting field for f over F. Let the zeros of f in K be $\alpha_1, \ldots, \alpha_n$. Let $\Delta(f) = \Pi_{i<j}(\alpha_i - \alpha_j)$. Show that $(\Delta(f))^2 \in F$.*

Consider the set S of automorphisms in $G(K/F)$ that leave $(\Delta(f))^2$ fixed. For any $\sigma \in G(K/F)$, we know that σ induces a permutation on the α_i, but $(\Delta(f))^2$ is a symmetric function in the α_i, so it is fixed by any permutation of the α_i. Therefore, $(\Delta(f))^2$ is in the fixed field of $G(K/F)$, which is F.