Algebra II - Homework 8

Pablo Sánchez Ocal

April 26th, 2017

Exercise 1

Let K be a field of characteristic zero, we define:

$$\begin{array}{rccc} \sigma & : & K(t) & \longrightarrow & K(t) \\ & & f(t) & \longmapsto & f\left(\frac{1}{-t}\right), \end{array} \qquad \begin{array}{rccc} \tau & : & K(t) & \longrightarrow & K(t) \\ & & f(t) & \longmapsto & f\left(t+1\right). \end{array}$$

1. We show that σ and τ are automorphisms of $K(t)$ over K. We first notice that for $\alpha \in K \subset K[x]$ we clearly have that $\sigma(\alpha) = \alpha = \tau(\alpha)$ hence $\sigma|_K = \mathrm{id}_K = \tau|_K$, meaning that if we prove that σ and τ are automorphisms of $K(t)$, we automatically obtain the desired result.

   Consider first $r, s \in K[t]$, say $r = \sum_{i=1}^n r_i t^i$, $s = \sum_{i=1}^n s_i t^i$ with $r_i, s_i \in K$ for $i = 1, \ldots, n$, we have:

$$\begin{aligned} \sigma(r+s) &= \sigma\left(\sum_{i=1}^n (r_i + s_i)t^i\right) = \sum_{i=1}^n (r_i + s_i)\left(\frac{1}{-t}\right)^i \\ &= \left(\sum_{i=1}^n r_i \left(\frac{1}{-t}\right)^i\right) + \left(\sum_{i=1}^n s_i \left(\frac{1}{-t}\right)^i\right) = \sigma(r) + \sigma(s), \\ \sigma(rs) &= \sigma\left(\sum_{i,j=1}^n r_i s_j t^{i+j}\right) = \sum_{i,j=1}^n r_i s_j \left(\frac{1}{-t}\right)^{i+j} \\ &= \left(\sum_{i=1}^n r_i \left(\frac{1}{-t}\right)^i\right)\left(\sum_{i=1}^n s_i \left(\frac{1}{-t}\right)^i\right) = \sigma(r)\sigma(s), \\ \tau(r+s) &= \tau\left(\sum_{i=1}^n (r_i + s_j)t^i\right) = \sum_{i=1}^n (r_i + s_i)(t+1)^i \\ &= \left(\sum_{i=1}^n r_i (t+1)^i\right) + \left(\sum_{i=1}^n s_i (t+1)^i\right) = \tau(r) + \tau(s), \\ \tau(rs) &= \tau\left(\sum_{i,j=1}^n r_i s_j t^{i+j}\right) = \sum_{i,j=1}^n r_i s_j (t+1)^{i+j} \\ &= \left(\sum_{i=1}^n r_i (t+1)^i\right)\left(\sum_{i=1}^n s_i (t+1)^i\right) = \tau(r)\tau(s). \end{aligned}$$

   If we now consider $f, g \in K(t)$, that is, $f = f_1/f_2$ and $g = g_1/g_2$ with $f_1, f_2, g_1, g_2 \in K[t]$ (say $f_1 = \sum_{i=1}^n f_{1,i}t^i$, $f_2 = \sum_{i=1}^n f_{2,i}t^i$, $g_1 = \sum_{i=1}^n g_{1,i}t^i$, $g_2 = \sum_{i=1}^n g_{2,i}t^i$ with

$f_{1,i}, f_{2,i}, g_{1,i}, g_{2,i} \in K$ for $i = 1, \ldots, n$, although this is not relevant), we have:

$$\begin{aligned}
\sigma(f+g) &= \sigma\left(\frac{f_1g_2+f_2g_1}{f_2g_2}\right) := \frac{\sigma(f_1g_2+f_2g_1)}{\sigma(f_2g_2)} = \frac{\sigma(f_1)\sigma(g_2)+\sigma(f_2)\sigma(g_1)}{\sigma(f_2)\sigma(g_2)} \\
&= \frac{\sigma(f_1)}{\sigma(f_2)} + \frac{\sigma(g_1)}{\sigma(g_2)} = \sigma(f) + \sigma(g), \\
\sigma(fg) &= \sigma\left(\frac{f_1g_1}{f_2g_2}\right) := \frac{\sigma(f_1g_1)}{\sigma(f_2g_2)} = \frac{\sigma(f_1)\sigma(g_1)}{\sigma(f_2)\sigma(g_2)} = \frac{\sigma(f_1)}{\sigma(f_2)}\frac{\sigma(g_1)}{\sigma(g_2)} = \sigma(f)\sigma(g), \\
\tau(f+g) &= \tau\left(\frac{f_1g_2+f_2g_1}{f_2g_2}\right) := \frac{\tau(f_1g_2+f_2g_1)}{\tau(f_2g_2)} = \frac{\tau(f_1)\tau(g_2)+\tau(f_2)\tau(g_1)}{\tau(f_2)\tau(g_2)} \\
&= \frac{\tau(f_1)}{\tau(f_2)} + \frac{\tau(g_1)}{\tau(g_2)} = \tau(f) + \tau(g), \\
\tau(fg) &= \tau\left(\frac{f_1g_1}{f_2g_2}\right) := \frac{\tau(f_1g_1)}{\tau(f_2g_2)} = \frac{\tau(f_1)\tau(g_1)}{\tau(f_2)\tau(g_2)} = \frac{\tau(f_1)}{\tau(f_2)}\frac{\tau(g_1)}{\tau(g_2)} = \tau(f)\tau(g),
\end{aligned}$$

which proves that σ and τ are morphisms. Consider now:

$$\begin{array}{rcccc}
\sigma' & : & K(t) & \longrightarrow & K(t) \\
 & & f(t) & \longmapsto & f\left(\frac{1}{-t}\right),
\end{array}
\qquad
\begin{array}{rcccc}
\tau' & : & K(t) & \longrightarrow & K(t) \\
 & & f(t) & \longmapsto & f\left(t-1\right).
\end{array}$$

We notice that the definition of σ, τ, σ' and τ' amounts to renaming the variable t in such a way that after a simplification we still obtain an element of $K(t)$. Thus composing this simplification again with σ, τ, σ' or τ' and undoing it amounts to successively renaming the variable t in the order of the composition. In fact, this holds for any such morphism that simply renames the variable t as above. Otherwise said, for γ and δ morphisms renaming the variable t in such a way that after a simplification we still obtain an element of $K(t)$ (in particular for σ, τ, σ' and τ') we have $\gamma \circ \delta(f(t)) = f(\gamma \circ \delta(t))$ (and since $\gamma \circ \delta(t)$ is a morphism that renames the variable t in such a way that after a simplification we still obtain an element of $K(t)$, this remains true for compositions of σ, τ, σ' and τ').

We have that $\sigma' = \sigma$ and:

$$\begin{aligned}
\tau'(r+s) &= \tau'\left(\sum_{i=1}^{n}(r_i+s_j)t^i\right) = \sum_{i=1}^{n}(r_i+s_i)\,(t-1)^i \\
&= \left(\sum_{i=1}^{n} r_i\,(t-1)^i\right) + \left(\sum_{i=1}^{n} s_i\,(t-1)^i\right) = \tau'(r) + \tau'(s), \\
\tau'(rs) &= \tau'\left(\sum_{i,j=1}^{n} r_is_jt^{i+j}\right) = \sum_{i,j=1}^{n} r_is_j\,(t-1)^{i+j} \\
&= \left(\sum_{i=1}^{n} r_i\,(t-1)^i\right)\left(\sum_{i=1}^{n} s_i\,(t-1)^i\right) = \tau'(r)\tau'(s),
\end{aligned}$$

and:

$$\begin{aligned}
\tau'(f+g) &= \tau'\left(\frac{f_1g_2+f_2g_1}{f_2g_2}\right) := \frac{\tau'(f_1g_2+f_2g_1)}{\tau'(f_2g_2)} = \frac{\tau'(f_1)\tau'(g_2)+\tau'(f_2)\tau'(g_1)}{\tau'(f_2)\tau'(g_2)} \\
&= \frac{\tau'(f_1)}{\tau'(f_2)} + \frac{\tau'(g_1)}{\tau'(g_2)} = \tau'(f)+\tau'(g), \\
\tau'(fg) &= \tau'\left(\frac{f_1g_1}{f_2g_2}\right) := \frac{\tau'(f_1g_1)}{\tau'(f_2g_2)} = \frac{\tau'(f_1)\tau'(g_1)}{\tau'(f_2)\tau'(g_2)} = \frac{\tau'(f_1)}{\tau'(f_2)}\frac{\tau'(g_1)}{\tau'(g_2)} = \tau'(f)\tau'(g),
\end{aligned}$$

which proves that σ' and τ' are morphisms. Since we have:

$$\begin{aligned}
\sigma\circ\sigma'(f(t)) &= f\left(\frac{-1}{-1/t}\right) = f(t) = \mathrm{id}_{K(t)}(f(t)), \\
\sigma'\circ\sigma(f(t)) &= f\left(\frac{-1}{-1/t}\right) = f(t) = \mathrm{id}_{K(t)}(f(t)), \\
\tau\circ\tau'(f(t)) &= f((t+1)-1) = f(t) = \mathrm{id}_{K(t)}(f(t)), \\
\tau'\circ\tau(f(t)) &= f((t-1)+1) = f(t) = \mathrm{id}_{K(t)}(f(t)),
\end{aligned}$$

this means that σ' and τ' are inverses of σ and τ, meaning that the latter are bijective and thus indeed automorphisms of $K(t)$.

2. As we saw in the section above, we have that $\sigma\circ\sigma = \mathrm{id}_{K(t)}$ and hence σ has order two. Moreover, considering $f(t) = t$ we have $f \in K[t] \subset K(t)$ and $\tau^n(f) = t+n$. Since K has characteristic zero, we have that $t+n \neq t$ for every $n \in \mathbb{N}\setminus\{0\}$, meaning that $\tau^n(f) \neq f$ for every $n \in \mathbb{N}\setminus\{0\}$, hence τ has infinite order.

3. We can compute the order of $\sigma\circ\tau$ by using that $\sigma\circ\tau(f(t)) = f(\sigma\circ\tau(t))$. We have:

$$\begin{aligned}
\sigma\circ\tau(f(t)) &= f\left(\frac{-1}{t}+1\right) = f\left(\frac{t-1}{t}\right) \neq f(t), \\
(\sigma\circ\tau)^2(f(t)) &= f\left(1-\frac{1}{1-1/t}\right) = f\left(1-\frac{t}{t-1}\right) = f\left(\frac{1}{1-t}\right) \neq f(t), \\
(\sigma\circ\tau)^3(f(t)) &= f\left(\frac{1}{1-(t-1)/t}\right) = f\left(\frac{-t}{-1}\right) = f(t),
\end{aligned}$$

and $\sigma\circ\tau$ has order three.

4. If we assume that K has characteristic two, notice how now $\tau^2(f(t)) = f((t+1)+1) = f(t+2) = f(t)$ and thus now τ has order two. This means that:

$$\begin{aligned}
\langle\sigma,\sigma\circ\tau\rangle &= \langle\sigma,\sigma\circ\tau|\sigma^2 = (\sigma\circ\tau)^3 = 1\rangle = \langle\sigma,\tau|\sigma^2=\tau^2=(\sigma\circ\tau)^3=1\rangle \\
&= \langle\sigma,\tau|\sigma^2=\tau^2=(\sigma\circ\tau)^3=\sigma\circ\tau\circ\sigma\circ\tau=1\rangle \cong D_3 \cong S_3
\end{aligned}$$

where the first equality is due to the computations above, the second equality is due to $\sigma \circ (\sigma \circ \tau) = \tau$, the third equality is due to:

$$\begin{aligned} \sigma \circ \tau \circ \sigma(f(t)) &= f(\sigma \circ \tau \circ \sigma(t)) = f\left(\sigma \circ \tau \left(\frac{-1}{t}\right)\right) \\ &= f\left(\sigma\left(\frac{-1}{t+1}\right)\right) = f\left(t+1\right) = \tau(f(t)) \end{aligned}$$

and τ being its own inverse, and the fourth equality is obtained applying [1, Theorem 6.13 (p. 50)] since the presentation above satisfies all the hypothesis. The last isomorphism can be obtained in multiple ways, one of them being the direct computation of their multiplication table, other being using the classification of finite groups (namely [1, Corollary 6.2 (p. 97)]).

Exercise 2

We show that towers of normal extensions need not be normal. For this, we consider the tower of fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$. We remark that from now on we will only deal with monic polynomials, and a monic polynomial splits if and only if it can be completely factorized into polynomials of degree 1.

Notice how $\mathbb{Q}(\sqrt[4]{2})$ is the splitting field of $x^2 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$ because we can write $x^2 - \sqrt{2} = (x - \sqrt[4]{2})(x + \sqrt[4]{2})$ with $\pm\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ and clearly $\mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2})$. Hence $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is normal.

Notice how $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$ because we can write $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ with $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ and clearly $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$. Hence $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal.

Moreover, notice that $x^4 - 2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion with the prime 2. It has solutions $s^2 = \pm\sqrt{2}$, that is, $s = \pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ and we have that $s, s^2 \notin \mathbb{Q}$. However, $x^4 - 2$ has the root $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$, but $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$ because $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ but $i\sqrt[4]{2} \notin \mathbb{R}$. Hence we found an irreducible polynomial in $\mathbb{Q}[x]$ with one root in $\mathbb{Q}(\sqrt[4]{2})$ but that does not split in $\mathbb{Q}(\sqrt[4]{2})$, meaning that $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal, providing the desired counterexample.

Exercise 3

1. We compute E the splitting field of x^4-2 over $\mathbb{Q}$ explicitly and determine $[E:\mathbb{Q}]$.

   First, the roots of x^4-2 are $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ as computed above. Hence we want $E = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$ since multiplying and dividing by elements of the field we can go from left to right without any issues, that is, adding the four roots to $\mathbb{Q}$ is equivalent to adding $\sqrt[4]{2}$ and i to $\mathbb{Q}$. The expression $E = \mathbb{Q}(\sqrt[4]{2}, i)$ is an explicit one (and it also solves the first part of the following section).

   It only remains to compute $[E:\mathbb{Q}]$. For this, we notice that $[E:\mathbb{Q}] = [E:\mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]$. We have already proven that x^4-2 is irreducible in $\mathbb{Q}[x]$ and annihilates $\sqrt[4]{2}$, hence $\mathrm{Irr}(\sqrt[4]{2}, \mathbb{Q}, x) = x^4-2$ meaning that $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = 4$. Moreover, we have that $x^2+1 \in \mathbb{Q}(\sqrt[4]{2})[x]$ annihilates i and has roots $s = \pm i \notin \mathbb{Q}(\sqrt[4]{2})$, meaning that it is irreducible in $\mathbb{Q}(\sqrt[4]{2})[x]$, hence $\mathrm{Irr}(i, \mathbb{Q}(\sqrt[4]{2}), x) = x^2+1$ meaning that $[E:\mathbb{Q}(\sqrt[4]{2})] = [\mathbb{Q}(\sqrt[4]{2})(i):\mathbb{Q}(\sqrt[4]{2})] = 2$. Finally, we have that $[E:\mathbb{Q}] = 2\cdot 4 = 8$.

2. We compute F the splitting field of x^4+4 over $\mathbb{Q}$ explicitly and determine $[F:\mathbb{Q}]$.

   First, we compute the roots of x^4+4. Setting $x^2 = y$ we have $y^2+4=0$ annihilated by $\pm i2$. Now $x^2 = i2$ is annihilated by $\pm\sqrt{i}\sqrt{2}$ and $x^2 = -i\sqrt{2}$ is annihilated by $\pm i\sqrt{i}\sqrt{2}$. Since $\sqrt{i} = e^{i\pi/4} = w$ the fourth root of unity, we have that the roots of x^4+4 are $\pm w\sqrt{2}$ and $\pm iw\sqrt{2}$. Moreover, we can use the exponential expressions $-1 = e^{i\pi}$, $i = e^{i\pi/2}$ and that $e^{i\theta} = \cos(\theta) + i\sin(\theta)$ to find:

$$\begin{aligned} w\sqrt{2} &= e^{i\pi/4}\sqrt{2} = 1+i, \\ iw\sqrt{2} &= e^{3i\pi/4}\sqrt{2} = -1+i, \\ -iw\sqrt{2} &= e^{7i\pi/4}\sqrt{2} = -1-i, \\ -w\sqrt{2} &= e^{5i\pi/4}\sqrt{2} = 1-i. \end{aligned}$$

   Hence we want $E = \mathbb{Q}(1+i, -1+i, -1-i, 1-i) = \mathbb{Q}(i)$ since multiplying and dividing by elements of the field we can go from left to right without any issues, that is, adding the four roots to $\mathbb{Q}$ is equivalent to adding i to $\mathbb{Q}$. The expression $F = \mathbb{Q}(i)$ is an explicit one.

   It only remains to compute $[F:\mathbb{Q}]$. For this, we notice that $x^2+1 \in \mathbb{Q}[x]$ annihilates i and has roots $s = \pm i \notin \mathbb{Q}$, meaning that it is irreducible in $\mathbb{Q}[x]$, hence $\mathrm{Irr}(i, \mathbb{Q}, x) = x^2+1$ meaning that $[F:\mathbb{Q}] = 2$.

Exercise 4

Let E be the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

1. Find $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{C}$ with $E = \mathbb{Q}(\alpha, \beta)$. As we have seen above, $\alpha = \sqrt[4]{2} \in \mathbb{R}$ and $\beta = i \in \mathbb{C}$ are as desired.

2. To determine all embedding of E into $\mathbb{C}$ over $\mathbb{Q}$, we will proceed as in the section above, first computing the embedding of $\mathbb{Q}(\sqrt[4]{2})$ into $\mathbb{C}$ over $\mathbb{Q}$ and then computing the embedding of $\mathbb{Q}(\sqrt[4]{2}, i)$ into $\mathbb{C}$ over $\mathbb{Q}(\sqrt[4]{2})$ given one of the computed above. For this, we will abuse the result we proved in class stating that given $\sigma : K \longrightarrow L$ an embedding with L algebraically closed, if $K(\alpha)/K$ is algebraic, then the number of embedding of $K(\alpha)$ into L preserving σ over K coincides with the number of distinct roots of $\mathrm{Irr}(\alpha, K, x)$ in some $\overline{K}$ (we actually use the construction in the proof that tells us that these embedding must permute the roots of $\mathrm{Irr}(\alpha, K, x)$, hence we can completely determine them by choosing where to send α).

   We computed above that $\mathrm{Irr}(\sqrt[4]{2}, \mathbb{Q}, x) = x^4 - 2$ with roots $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ and $\mathrm{Irr}(i, \mathbb{Q}(\sqrt[4]{2}), x) = x^2 + 1$ with roots $\pm i$. Thus by the discussion above we have:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[4]{2}, i) & \xrightarrow{\rho_\tau} & \mathbb{C} \\ | & & | \\ \mathbb{Q}(\sqrt[4]{2}) & \xrightarrow{\tau} & \mathbb{C} \\ | & & | \\ \mathbb{Q} & \xrightarrow{\mathrm{id}_{\mathbb{Q}}} & \mathbb{C} \end{array}$$

   with four possible choices for τ (the images of $\sqrt[4]{2}$) and two possible choices for ρ_τ (the images of i), meaning that we will have a total of eight embedding. Choosing $\sqrt[4]{2}$ and i as images, we obtain:

$$\begin{array}{rccc} \rho & : & \mathbb{Q}(\sqrt[4]{2}, i) & \longrightarrow & \mathbb{C} \\ & & \sqrt[4]{2} & \longmapsto & \sqrt[4]{2}. \\ & & i & \longmapsto & i \end{array}$$

   Choosing $-\sqrt[4]{2}$ and i as images, we obtain:

$$\begin{array}{rccc} \rho & : & \mathbb{Q}(\sqrt[4]{2}, i) & \longrightarrow & \mathbb{C} \\ & & \sqrt[4]{2} & \longmapsto & -\sqrt[4]{2}. \\ & & i & \longmapsto & i \end{array}$$

   Choosing $i\sqrt[4]{2}$ and i as images, we obtain:

$$\begin{array}{rccc} \rho & : & \mathbb{Q}(\sqrt[4]{2}, i) & \longrightarrow & \mathbb{C} \\ & & \sqrt[4]{2} & \longmapsto & i\sqrt[4]{2}. \\ & & i & \longmapsto & i \end{array}$$

Choosing $-i\sqrt[4]{2}$ and i as images, we obtain:

$$\begin{array}{rccc} \rho & : & \mathbb{Q}(\sqrt[4]{2}, i) & \longrightarrow & \mathbb{C} \\ & & \sqrt[4]{2} & \longmapsto & -i\sqrt[4]{2}. \\ & & i & \longmapsto & i \end{array}$$

Choosing $\sqrt[4]{2}$ and $-i$ as images, we obtain:

$$\begin{array}{rccc} \rho & : & \mathbb{Q}(\sqrt[4]{2}, i) & \longrightarrow & \mathbb{C} \\ & & \sqrt[4]{2} & \longmapsto & \sqrt[4]{2}. \\ & & i & \longmapsto & -i \end{array}$$

Choosing $-\sqrt[4]{2}$ and $-i$ as images, we obtain:

$$\begin{array}{rccc} \rho & : & \mathbb{Q}(\sqrt[4]{2}, i) & \longrightarrow & \mathbb{C} \\ & & \sqrt[4]{2} & \longmapsto & -\sqrt[4]{2}. \\ & & i & \longmapsto & -i \end{array}$$

Choosing $i\sqrt[4]{2}$ and $-i$ as images, we obtain:

$$\begin{array}{rccc} \rho & : & \mathbb{Q}(\sqrt[4]{2}, i) & \longrightarrow & \mathbb{C} \\ & & \sqrt[4]{2} & \longmapsto & i\sqrt[4]{2}. \\ & & i & \longmapsto & -i \end{array}$$

Choosing $-i\sqrt[4]{2}$ and $-i$ as images, we obtain:

$$\begin{array}{rccc} \rho & : & \mathbb{Q}(\sqrt[4]{2}, i) & \longrightarrow & \mathbb{C} \\ & & \sqrt[4]{2} & \longmapsto & -i\sqrt[4]{2}. \\ & & i & \longmapsto & -i \end{array}$$

These are the explicit expressions of the eight embedding operating on $\alpha = \sqrt[4]{2} \in \mathbb{R}$ and $\beta = i\sqrt[4]{2} \in \mathbb{C}$ are as desired.

References

[1] T. W. Hungerford, *Algebra*, Springer-Verlag, 2000.