Math 504, Fall 2013
HW 3

1. Let $F = \mathbb{F}_2(x)$ be the field of rational functions over the field of order 2. Show that the extension $K = F(x^{1/6})$ of F is equal to $F(\sqrt{x}, x^{1/3})$. Show that $F(x^{1/3})$ is separable over F. Show that $F(\sqrt{x})$ is purely inseparable over F.

We first show that $F(x^{1/6}) = F(\sqrt{x}, x^{1/3})$. Note that $(x^{1/6})^3 = \sqrt{x}$ and $(x^{1/6})^2 = x^{1/3}$, so $F(\sqrt{x}, x^{1/3}) \subset F(x^{1/6})$. Since $F(\sqrt{x}, x^{1/3})$ contains $x^{1/3}$ and is a field, it contains $x^{-1/3}$. $x^{1/2} \times x^{-1/3} = x^{1/6}$, so $x^{1/6} \in F(\sqrt{x}, x^{1/3})$ so $F(x^{1/6}) \subset F(\sqrt{x}, x^{1/3})$. We conclude that $F(x^{1/6}) = F(\sqrt{x}, x^{1/3})$.

We know that an extension is separable if every generator is, therefore it suffices to show that the minimal polynomial of $x^{1/3}$ is separable. Note that the minimal polynomial of $x^{1/3}$ over F is $f(y) = y^3 - x$. This has $f'(y) = 3y^2 = y^2 \neq 0$. Because $f' \neq 0$ f is separable. Because $F(x^{1/3})$ is generated by separable elements it is a separable extension.

The minimal polynomial of $x^{1/2}$ over F is $f(y) = y^2 - x$. Then $f'(y) = 2y = 0$ so $x^{1/2}$ is not separable. Because it is a polynomial of degree two this implies that f has only one root. Furthermore, because $(x^{1/2})^2 = x \in F(x)$, we can reduce any polynomial of larger degree to a polynomial of degree 1 or 2, so no non-linear polynomial will split into a product of linear factors in $F(x^{1/2})$ so $F(x^{1/2})$ is purely inseparable. ∎

COMMENTS: If one wants to be very precise, it's worth to point out that although for every element of F there's only one square root, there are three sixth roots of x, and three cube roots of x. Hence, if we denote by $x^{1/6}$ a sixth root of x, then $(x^{1/6})^2$ is one of the cube roots of x. Therefore if we want the inclusion $F(x^{1/3}) \subseteq F(x^{1/6})$ we need a "compatible" choice of roots of x.

2. Find the degree of the splitting field over $\mathbb{Q}$ for the following polynomials: $x^4 - 1$, $x^4 + 1$, $x^4 + 2$, $x^4 + 4$.

Let L denote the splitting field of the given polynomial $f(x) \in \mathbb{Q}[x]$.

1. $f(x) = x^4 - 1 = (x-1)(x+1)(x^2+1) = \Phi_1(x)\Phi_2(x)\Phi_4(x)$. This polynomial already has two of its roots in $\mathbb{Q}$, the only ones remaining are the roots from the irreducible (rational roots) quadratic $x^2 + 1$. Actually we know the splitting field of this is the fourth roots of unity $\pm i, \pm 1$. The extension $L = \mathbb{Q}(i)$ is thus of degree two.

2. $f(x) = x^4 + 1$. Using complex arithmetic, we find the roots of $f(x)$ are

$$\{e^{i\pi/4}, e^{3i\pi/4}, e^{5i\pi/4}, e^{7i\pi/4}\},$$

and by Euler's formula, the roots turn out to be $\{\pm\frac{1}{\sqrt{2}} \pm i\frac{1}{\sqrt{2}}\}$. The field $\mathbb{Q}(e^{i\pi/4}) \supset L$, since powers of $e^{i\pi/4}$ generate the other three roots of x^4+1, and we also have $i, \sqrt{2} \in L$ by adding and subtracting the roots. But $\mathbb{Q}(e^{i\pi/4}) = \mathbb{Q}(i, \sqrt{2})$ since $(e^{i\pi/4})^2 = i$ and $(e^{i\pi/4})^3 = -\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$ imply $i, \sqrt{2} \in \mathbb{Q}(e^{i\pi/4})$. But then we may conclude $\mathbb{Q}(i, \sqrt{2}) \subset L$ by minimality since $i, \sqrt{2} \in L$. Now since $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ and since $\mathbb{Q}(\sqrt{2})$ is contained in $\mathbb{R}$ but $\mathbb{Q}(i, \sqrt{2})$ is not, we conclude that both the extensions have degree 2 and therefore $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$. It follows that $[L : \mathbb{Q}] = 4$.

3. $f(x) = x^4 + 2$. First, this polynomial is irreducible by Eisenstein at $p = 2$. Again by Euler's formula, the roots are $\frac{1}{\sqrt[4]{2}}(\pm 1 \pm i)$. Clearly $L \supset \mathbb{Q}(i, \sqrt[4]{2})$, whence $[L : \mathbb{Q}] \leq 8$ because $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ and this field is real, so $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$ (see problem 4 for more details). But since $\frac{1}{\sqrt[4]{2}}(1 \pm i) \in L$, we have $\mathbb{Q}(\sqrt[4]{2}) \subset L$ (since $(2^{3/4})^3 = 4\sqrt[4]{2}$), thus $[L : \mathbb{Q}] > 4$, since L contains a purely real quartic extension. By the tower property, we must divide 8, and thus we have $[L : \mathbb{Q}] = 8$, as desired.

4. We note that $f(x) = x^4 + 4$ factors over $\mathbb{Q}$, since $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$, and by the quadratic formula, the roots are $\pm 1 \pm i$, so $[L : \mathbb{Q}] = 2$.

$\blacksquare$

3. Find the degree of the splitting field for $x^6 + 1$ over $\mathbb{Q}$ and $\mathbb{F}_2$.

Over $\mathbb{Q}$:

Let $\omega = e^{\pi i/6}$. Then the roots of $x^6 + 1$ are obviously $\pm i, \pm\omega, \pm\omega^5$, so the splitting field of $x^6 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(i, \omega, \omega^5) = \mathbb{Q}(i, \omega)$.

In Cartesian form, we have:

$$\omega = \frac{\sqrt{3} + i}{2}$$

Consequently, $\mathbb{Q}(i, \omega) = \mathbb{Q}(i, 2\omega - i) = \mathbb{Q}(i, \sqrt{3})$.

Now, $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ because $\sqrt{3}$ is not rational and has minimal polynomial $x^2 - 3$ (irreducible by Eisenstein). Furthermore, $\mathbb{Q}(\sqrt{3})$ is a real extension of $\mathbb{Q}$, so it does not contain i. Thus, $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] > 1$, and $[\mathbb{Q}(\sqrt{3}, i)\mathbb{Q}(\sqrt{3})] \leq 2$ because $x^2 + 1 \in \mathbb{Q}(\sqrt{3})[x]$ is satisfied by i, so $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})] = 2$. Finally, $[\mathbb{Q}(i, \omega) : \mathbb{Q}] = 4$ by multiplicativity of degrees.

Over $\mathbb{F}_2$:

First, note that $x^6 + 1 = (x^3 + 1)^2$, so it is sufficient to find a splitting field for $x^3 + 1$. Furthermore, $x^3 + 1 = (x + 1)(x^2 - x + 1)$. The polynomial $x^2 - x + 1$ is irreducible over

$\mathbb{F}_2$, because $0^2 - 0 + 1 = 1^2 - 1 + 1 = 1 \neq 0$, which shows it has no roots in $\mathbb{F}_2$. Let α be a root of $x^2 + x + 1$ in some field extension of $\mathbb{F}_2$. Compute that:

$$(\alpha+1)^2 - (\alpha+1) + 1 = \alpha^2 + 1 - \alpha - 1 + 1 = \alpha^2 - \alpha + 1 = 0$$

Thus, it's clear that:

$$x^6 + 1 = (x-1)^2(x-\alpha)^2(x-\alpha-1)^2$$

so a splitting field for $x^6 + 1$ is $\mathbb{F}_2[\alpha]$, which has degree 2.

■

4. Show that the extension of $\mathbb{Q}$ generated by a root of $x^4 - 2$ is not normal. Deduce that a normal extension of a normal extension need not be normal.

First, note that:

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

Next, note that:

$$K = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$$

K is clearly the splitting field of $x^4 - 2$ over $\mathbb{Q}$, because it is generated by the four roots of $x^4 - 2$. The equalities in the display obviously hold because $i \in \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ and $i\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2}, i)$.

Now, clearly $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$, because $\sqrt[4]{2}$ is a root of $x^4 - 2$, which is irreducible by Eisenstein ($p = 2$). Furthermore, this is a purely real extension, so $i \notin \mathbb{Q}(\sqrt[4]{2})$. Thus, $[K : \mathbb{Q}(\sqrt[4]{2})] > 1$ because we need to adjoin i, and i satisfies $x^2 + 1$, so $[K : \mathbb{Q}(\sqrt[4]{2})] = 2$ and $[K : \mathbb{Q}] = 8$.

If α is a root of $x^4 - 2$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ because $x^4 - 2$ is irreducible, so $\mathbb{Q}(\alpha) \neq K$.

Thus, we conclude that a normal extension of a normal extension need not be normal. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is certainly normal, because it is the splitting field of $x^2 - 2$. Furthermore, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ is normal, because it is the splitting field of $x^2 - \sqrt{2}$. However, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal by the proof above.

■

5. If a field of characteristic p has n distinct n^{th} roots of unity show that p does not divide n.

Suppose that k is a field of characteristic p that has n distinct n-th roots of unity. Then, the polynomial $f(x) = x^n - 1$ has n distinct roots, hence $f(x)$ has no repeated roots, meaning that $f'(x) \neq 0$. So,

$$f'(x) = nx^{n-1} \neq 0$$

If p did divide n, we would have $n = 0$ and $f'(x) = 0$, contradicting the above. Hence, p does not divide n. ■

6. Let K be a perfect field, and G be the group of all automorphisms of K. Show that the invarient subfield K^G is perfect.

We can assume char $K = p > 0$, otherwise it's trivial. Since K is perfect, every element of K is a pth power, so the Frobenius endomorphism

$$\mathrm{Frob}_p \colon x \mapsto x^p$$

is surjective on K, so it is an automorphism.

Then K^G is pointwise fixed by Frob_p, so for any $y \in K^G$, $y^p = y$ so y is a pth power. Thus K^G is perfect. It's worth to observe that K^G consists of the roots of $x^p - x$, hence it coincides with the prime subfield $\mathbb{F}_p$. ∎

7. Let x be trancendental over a field k. Show that $k(x)$ is a degree 6 extension of $k(x)^G$ where G is the group generated by the automorphisms $x \to x^{-1}$ and $x \to 1 - x$. Show that $(x^2 - x + 1)^3/(x^2 - x)^2$ is in $k(x)^G$. and use that to compute the minimal polynomial of x over $k(x)^G$.

Let $\varphi : x \mapsto 1/x$ and $\psi : x \mapsto 1 - x$ be the automorphisms of $k(x)$ that generate G. Let $z = \frac{(x^2-x+1)^3}{(x^2-x)^2} \in k(x)$. We have

$$\begin{aligned}\varphi(z) &= \frac{(x^{-2} - x^{-1} + 1)^3}{(x^{-2} + x^{-1})^2} \\ &= \frac{(1 - x + x^2)^3}{(-x + x^2)^2} \cdot \frac{x^{-6}}{x^{-6}} \\ &= z\end{aligned}$$

and

$$\begin{aligned}\psi(z) &= \psi\left(\frac{(x(1-x)+1)^3}{x^2(1-x)^2}\right) \\ &= z.\end{aligned}$$

Therefore z is fixed under the action of G, so $z \in k(x)^G$. Now consider the degree 6 polynomial in $k(x)^G[t]$ given by

$$p(t) = (t^2 - t + 1)^3 + (t^2 - t)^2 z.$$

Clearly $p(x) = 0$, so $[k(x) : k(x)^G] \le 6$.

On the other hand, the orbit of x under G has at least 6 distinct elements (we actually have that G is isomorphic to S_3 but this will not be needed in the proof). In particular,

$$\begin{gathered}\varphi x = \frac{1}{x}, \quad \psi x = 1 - x, \quad \varphi\psi x = \frac{1}{1-x} \\ \psi\varphi\psi x = \frac{x}{x-1}, \quad \psi\varphi x = \frac{x-1}{x}, \quad \mathrm{id}_G x = x.\end{gathered}$$

Now suppose $q(t) \in k(x)^G[t]$ is an irreducible polynomial satisfying $q(x) = 0$, in $k(x)$. Then for any $\mu \in G$ we must have that $\mu(q(x)) = q(\mu(x)) = 0$. Therefore q has at least 6 roots in $k(x)$ which means the degree of q is at least 6. Therefore the polynomial $p(t)$ is the miminal polynomial of x over $k(x)^G$ and in particular $[k(x) : k(x)^G] = 6$. ■

8. Show that $\mathbb{Q}(\sqrt{2}, 2^{1/3}) = \mathbb{Q}(\sqrt{2} + 2^{1/3})$.

We would like to show that the fields $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ and $\mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$ are equal. First note that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ is equal to $\mathbb{Q}(\sqrt[6]{2})$. The former is contained in the latter because $\sqrt{2} = (\sqrt[6]{2})^3$ and $\sqrt[3]{2} = (\sqrt[6]{2})^2$. But also $(\sqrt[3]{2})^2\sqrt{2} = 2^{7/6}$, so $\sqrt[6]{2}$ is in $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ and the fields are equal. Since $x^6 - 2$ is irreducible by Eisenstein's criterion, $\mathbb{Q}(\sqrt[6]{2})$ is a degree 6 extension of $\mathbb{Q}$.

It's immediate that $\mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$ is a subfield of $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, so the degree of the extension $\mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$ over $\mathbb{Q}$ is either 2, 3, or 6 (it must divide 6). Our result will then be proved if we can show that it is not a degree 2 or 3 extension, as this implies that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ is a degree 1 extension of $\mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$.

A basis for $\mathbb{Q}(\sqrt[6]{2})$ as a $\mathbb{Q}$-vector space is given by the powers of $\sqrt[6]{2}$ ranging from 0 to 5 (this is a result of problem (5) from the last homework). Now look at the powers of $\sqrt{2} + \sqrt[3]{2}$:

$$(\sqrt{2} + \sqrt[3]{2})^2 = 2 + 2\sqrt{2}\sqrt[3]{2} + (\sqrt[3]{2})^2 = 2 + 2(\sqrt[6]{2})^5 + (\sqrt[6]{4})^4$$
$$(\sqrt{2} + \sqrt[3]{2})^3 = 2 + 6(\sqrt[6]{2}) + 6(\sqrt[6]{2})^2 + 2(\sqrt[6]{2})^3$$

These powers of $\sqrt[6]{2}$ imply that the minimal polynomial for $\sqrt{2} + \sqrt[3]{2}$ cannot be a quadratic or a cubic; such a polynomial would provide a linear dependence among the powers of $\sqrt[6]{2}$, since the power $(\sqrt[6]{2})^5$ would occur only in the $(\sqrt{2} + \sqrt[3]{2})^2$ term while the power $\sqrt[6]{2}$ would occur only in the $(\sqrt{2} + \sqrt[3]{2})^3$ term. In short, any $\mathbb{Q}$-linear combinations of these cannot be zero unless all of the coefficients are zero. Hence, $\mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$ is a degree 6 extension of $\mathbb{Q}$ and it must be equal to $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. ■

9. Find the smallest normal extension of $\mathbb{Q}$ that contains $\sin(\pi/5)$.

We seek the smallest normal extension of $\mathbb{Q}$ containing $\sin\frac{\pi}{5} = \sqrt{\frac{5}{8} - \frac{\sqrt{5}}{8}}$. If we denote the right-hand side by t, then $8t^2 = 5 - \sqrt{5}$, whence $(8t^2 - 5)^2 - 5 = 64t^4 - 80t^2 + 20 = 0$. Therefore $m_{t,\mathbb{Q}}(x) \mid f(x) := x^4 - \frac{5}{4}x^2 + \frac{5}{16}$, but this polynomial is irreducible over $\mathbb{Q}$ as one can easily wee by clearing the denominators and then using Eisenstein's criterion.

By the quadratic formula (viewing this as a polynomial in x^2 then solving for x by square roots), the zeros are found to be $\pm\frac{1}{2}\sqrt{\frac{1}{2}(5 \pm \sqrt{5})}$. If we consider the *normal* extension of $\mathbb{Q}$ obtained by as a splitting field of the polynomial $x^4 - \frac{5}{4}x^2 + \frac{5}{16}$ over $\mathbb{Q}$, we generate, what we proceed to show, a degree 4 extension of $\mathbb{Q}$ containing $\sin(\pi/5)$. By the preceding paragraph, $[\mathbb{Q}(\sin(\pi/5)) : \mathbb{Q}] = 4$, and this extension generates at least two of the zeros of $f(x)$. If we let the roots be denoted by $\pm\alpha$ and $\pm\beta$ (where $\sin(\pi/5) = \alpha$, say), then we have so far that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. But note that $\alpha\beta = \frac{\sqrt{5}}{4}$ and further note $\alpha^2 = \frac{1}{8}(5 - \sqrt{5})$, whence $\sqrt{5} \in \mathbb{Q}(\alpha)$ and thus $\beta \in \mathbb{Q}(\alpha)$. Thus $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \beta)$ is a degree four normal extension of $\mathbb{Q}$. Any other extension containing $\alpha = \sin(\pi/5)$ must necessarily have degree at least 4, since $m_{\alpha,\mathbb{Q}}(x) = f(x)$, a degree four polynomial. Thus this is indeed the smallest normal extension of $\mathbb{Q}$ containing $\sin(\pi/5)$. ∎

10. Give an algebraic proof that every angle can be bisected by using a ruler and compass.

To do this, we will situate that angle in $\mathbb{C} \cong \mathbb{R}^2$, then this is equivalent to the following task: given the point $e^{i\theta} = (\cos\theta, \sin\theta)$, construct $e^{\frac{i\theta}{2}} = (\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$. We know that if we can individually construct $(\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$ from $(\cos\theta, \sin\theta)$, then this will be sufficient.

By the double-angle formula, we have that $\cos\theta = 2\cos^2\frac{\theta}{2} - 1$, or $\cos\theta + 1 = 2\cos^2\frac{\theta}{2}$. Since we can construct the $\cos\theta$, we can construct $\frac{\cos\theta+1}{2}$. To take the square root, given a segment of length a, we can construct a segment of length $\sqrt{a}$, and hence this gives us $\cos\frac{\theta}{2}$ as required. For $\sin\frac{\theta}{2}$, we know that $\sin\theta = 2\cos\frac{\theta}{2}\sin\frac{\theta}{2}$, and we know $\sin\theta$ and $\cos\frac{\theta}{2}$, hence we can construct $\sin\frac{\theta}{2}$.

Therefore, we can bisect any angle with a ruler and compass.

∎