Math 504, Fall 2013
HW 2

1. Show that the fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{7})$ are not isomorphic.

Suppose $\varphi : \mathbb{Q}(\sqrt{5}) \to \mathbb{Q}(\sqrt{7})$ is a field isomorphism. Then it's easy to see that φ fixes $\mathbb{Q}$ pointwise, so $5 = \varphi(5) = \varphi(\sqrt{5}\sqrt{5}) = \varphi(\sqrt{5})^2$, showing $\sqrt{5} \in \mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} : a, b \in \mathbb{Q}\}$. Thus

$$\sqrt{5} \;=\; a + b\sqrt{7} \tag{1}$$

for some rational a and b, and squaring yields

$$5 \;=\; a^2 + 7b^2 + 2ab\sqrt{7} \qquad \text{or} \qquad \frac{5 - a^2 - 7b^2}{2} \;=\; ab\sqrt{7}.$$

Thus either $a = 0$ or $b = 0$, because otherwise $\sqrt{7} \in \mathbb{Q}$. If $a = 0$ then (1) says that $\sqrt{5}$ is a rational multiple of $\sqrt{7}$, which is not the case. If $b = 0$ then $\sqrt{5} \in \mathbb{Q}$ according to (1). Either alternative is absurd, so there is no such isomorphism.

■

2. Let $\mathbb{F}_{11}$ be the field with 11 elements. Let $K = F_{11}(\alpha)$ where α is a root of $x^2 - 2$. Let $L = \mathbb{F}_{11}(\beta)$ where β is a root of $x^2 - 4x + 2$. Show that there is an isomorphism $\Phi : K \to L$ that is the identity in F_{11}.

Let $p(x) = x^2 - 2, q(x) = x^2 - 4x + 2$. Since both polynomials are irreducible in $\mathbb{F}_{11}[x]$, then we have

$$K = \mathbb{F}_{11}[x]/(p(x)), \quad L = \mathbb{F}_{11}[x]/(q(x))$$

Consider the automorphism f of $\mathbb{F}_{11}[x]$ given by $x \mapsto x - 2$, and let F be the composition of f with the projection $\mathbb{F}_{11}[x] \to L$. Since

$$F(p(x)) = (x-2)^2 - 2 = q(x) = 0$$

then F factors through a morphism $\Phi : K \to L$. This is a morphism of fields, hence injective. Since both K, L are finite fields, then it has to be bijective, hence it's the desired isomorphism. Moreover, since it's a composition of $\mathbb{F}_{11}$-linear maps, and since $\Phi(1) = 1$, then Φ is the identity on $\mathbb{F}_{11}$. ■

3. Let K/k a degree-two field extension. If $\mathrm{char}(k) \neq 2$, show that $K = k(\alpha)$ where α is a root of a polynomial $x^2 - d$ for some $d \in k$. Show this fails in characteristic two.

Complete the set $\{1\}$ to a basis $\{1, \beta\}$: clearly $\beta \notin k$ and also

$$\beta^2 = -a\beta - b$$

for some $a, b \in k$. Moreover, the extension $k(\beta)$ has degree at least two, and since $k(\beta) \subseteq K$ and K/k has degree 2, then $k(\beta) = K$ and K can be obtained by adding a root of $f(x) = x^2 + ax + b$ to k.

Our reasoning up to now holds in any characteristic, but now assume $\text{char}(k) \neq 2$. The idea is to use the quadratic formula to see that what we need to add to k to get K is indeed a square root.

Let α be a root of $x^2 - (a^2/4 - b)$. Then a straightforward computation shows that $f(\alpha - 2) = 0$, so $k(\alpha - 2) = k(\beta)$. Since clearly $k(\alpha - 2) = k(\alpha)$, then by letting $d = a^2/4 - b$ we have found what we were looking for.

This doesn't work in characteristic 2 because of the following example. Consider $k = \mathbb{F}_2$ and $K = k[x]/(x^2 - x - 1)$, whence $K = \{0, 1, \alpha, \alpha + 1\}$ where α is a root of $x^2 - x - 1$. The only polynomials of the form $x^2 - d$ for $d \in k$ are x^2 and $x^2 + 1$. Substituting α in to these polynomials yields $\alpha + 1$ and α, respectively. Since neither vanishes, α can not be a root of any polynomial of the form $x^2 - d$.

■

4. Let K/k be a degree-two field extension and suppose that $\text{char}(k) = 2$. Show that $K = k(\beta)$ where β is a root of a polynomial $x^2 + x + d$ or $x^2 - d$ for some $d \in k$.

From the previous Exercise, we have $K = k(\alpha)$ where $\alpha^2 = k_1\alpha + k_2$. If $k_1 = 0$, then α satisfies $x^2 - k_2 = 0$, which is the second polynomial.

Otherwise, $k_1 \neq 0$. Since k is a field, we have $\beta = \alpha/k_1 \in k$. Moreover,

$$\begin{aligned} (k_1\beta)^2 &= k_1^2\beta + k_2 = 0 \\ \implies \beta^2 &= \beta + k_2k_1^{-2} = 0 \\ \implies \beta^2 &+ \beta + d = 0 \end{aligned}$$

where $d = k_2k_1^{-2} \in k$. Clearly $K = k(\beta)$ and β satisfies $x^2 + x + d = 0$. ■

5. Let f be a polynomial of degree n in $k[x]$. Show that the images of $1, x, \ldots x^{n-1}$ in $k[x]/(f)$ form a basis for $k[x]/(f)$.

To show that $B := \{x^i\}_{i=0}^{n-1}$ is a basis, we'll start by showing it is linearly independent in $R = k[x]/(f)$. Indeed, suppose for some $a_i \in k$, we had

$$\sum_{i=0}^{n-1} (a_i + (f))(x^i + (f)) = 0 + (f)$$

Then we would have

$$f \mid g := \sum_{i=0}^{n-1} a_i x^i$$

But $\deg(f) = n > n-1 \geq \deg(g)$, so $g = 0$. This means each $\sum a_i x^i = 0$ in $k[x]$, and this forces $a_i = 0$. So we have shown linear independence.

Now, pick any (nonzero) coset $p + (f) \in R$. By polynomial division, we can write $p = af + b$, where $\deg(b) < \deg(f) = n$. So we may write $b = \sum_{i=0}^{n-1} a_i x^i$. But then

$$p + (f) = (af + b) + (f) = b + (f) = \sum_{i=0}^{n-1} (a_i + (f))(x^i + (f))$$

so we have shown B spans R, therefore it's a basis over k for R. ■

6. Find the minimal polynomial of $\sqrt{3} + \sqrt{5}$ over the fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{10})$, and $\mathbb{Q}(\sqrt{15})$.

We compute the minimal polynomial of $t = \sqrt{3} + \sqrt{5}$ over different fields $K \supset \mathbb{Q}$. We use the fact that $[K(t) : K] = \deg m_{t,K}(x)$

1. $K = \mathbb{Q}$.
   Since $t^2 = 8 + 2\sqrt{15}$, we have $t^2 - 8 = 2\sqrt{15}$ and squaring both sides we obtain $(t^2 - 8)^2 - 60 = 0$. Therefore $\deg m_{t,K}(x) \leq 4$. But since $t^2 = 8 + 2\sqrt{15}$, it follows $\mathbb{Q}(\sqrt{15}) \subset K(t)$, and since $[\mathbb{Q}(\sqrt{15}) : \mathbb{Q}] = 2$, we have $[K(t) : \mathbb{Q}]$ is even. But since $\sqrt{15}t - 3t = 3\sqrt{5} + 5\sqrt{3} - 3(\sqrt{3} + \sqrt{5}) = 2\sqrt{3}$, we must have $\mathbb{Q}(\sqrt{3}) \subset K(t)$. Finally, since the equation $\sqrt{3} = a + b\sqrt{15}$ cannot be solved for $a, b \in \mathbb{Q}$ (which can be seen by squaring the equation), it follows $\sqrt{3} \notin \mathbb{Q}(\sqrt{15})$, whence $[K(t) : \mathbb{Q}] \geq 4$, and we deduce $[K(t) : \mathbb{Q}] = 4 = \deg m_{t,K}$. Since $(t^2 - 8)^2 - 15$ is a degree four polynomial in $K[x]$, it follows by the division algorithm and the equality of degrees that $m_{t,K}(x)$ and $(x^2 - 8)^2 - 15$ are associates in $K[x]$. Since they are both monic, the constant must be one, and the result follows.

2. $K = \mathbb{Q}(\sqrt{3})$
   Since $(t - \sqrt{3}) = 5$, we have $x^2 - 2\sqrt{3}x - 2 \in K[x]$ has t as a root. Hence $\deg m_{t,K}(x) \leq 2$. If the degree was 1, we would have $t \in K$. But if $t \in K$, then $t - \sqrt{3} = \sqrt{5} \in K$. Since $\sqrt{5} = a + b\sqrt{3}$ cannot be solved with $a, b \in \mathbb{Q}$ (again seen most readily by squaring the equation), it follows $[K(t) : K] \geq 2$. By the same argument as in part (a), we obtain $m_{t,K}(x) = x^2 - 2\sqrt{3}x - 2$.

3. $K = \mathbb{Q}(\sqrt{10})$.
   Since $t^2 = 8 + 2\sqrt{15}$, we have $t^2 - 8 = 2\sqrt{15}$ and squaring both sides we obtain $(t^2 - 8)^2 - 60 = 0$. Therefore $\deg m_{t,K}(x) \leq 4$. But since $t^2 = 8 + 2\sqrt{15}$, it follows $\sqrt{15} \in K(t)$. But by checking whether $\sqrt{15} = a + b\sqrt{10}$ for rational a, b, we find $[K(\sqrt{15}) : K] = 2$, so that $[K(t) : K]$ is even. If $[K(t) : K] = 2$, the equation

$$[K(t) : \mathbb{Q}] = [K(t) : K][K : \mathbb{Q}] = 4$$

tells us the degree of $K(t)/\mathbb{Q}$. However, since $t = \sqrt{3} + \sqrt{5}$, the inverse t^{-1}, which can be computed by rationalizing the denominator, is $t^{-1} = \frac{-1}{2}(\sqrt{3} - \sqrt{5})$. Therefore we can linearly combine t and its inverse and we obtain $\sqrt{3}$ and $\sqrt{5}$ are both in $K(t)$. Since $\mathbb{Q}(\sqrt{10}, \sqrt{5}, \sqrt{3})$ is the smallest field containing all three, and since $\sqrt{2} = \sqrt{10}/\sqrt{5}$, we see $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subset K(t)$ again by minimality. But this is a degree 8 extension since the minimal polynomials are $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2, m_{\sqrt{3},\mathbb{Q}(\sqrt{2})} = x^2 - 3, m_{\sqrt{5},\mathbb{Q}(\sqrt{2},\sqrt{3})} = x^2 - 5$ (each is irreducible by basically the same argument of trying to write $\sqrt{5} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, squaring and moving the rationals to one side and concluding at least one of the coefficients must be zero... and then doing it again). Therefore we finally conclude $m_{t,\mathbb{Q}(\sqrt{10})} = (x^2 - 8)^2 - 60$.

4. $K = \mathbb{Q}(\sqrt{15})$.
   Since $t^2 = 8 + 2\sqrt{15}$, we have $x^2 - 8 - \sqrt{15} \in K[x]$ has t has a zero. Therefore $\deg m_{t,K}(x) \leq 2$. If it were strictly less, then $t \in K$. But if $t \in K$, then $\sqrt{15}t = 3\sqrt{5} + 15 \in K$ whence $\sqrt{5} \in K$. But since $\sqrt{5} = a + b\sqrt{15}$ has no solutions for $a, b \in \mathbb{Q}$, we obtain $[K(t) : K] \geq 2$, whence, mimicking the arguments in the previous parts, $m_{t,K}(x) = x^2 - 8 - \sqrt{15}$.

$\blacksquare$

7. Let f and g be non-zero polynomials in $k[x]$ and write z for $f(x)/g(x)$ which is an element in the field $k(x)$. Compute $[k(x) : k(z)]$.

First of all, note that we can assume that f, g are coprime in $k[x]$. Let $n = \deg f, m = \deg g$. Let us begin by examining the case $z \in k$, that is $n = m = 0$. Then we have to compute the degree of the extension $k(x)/k$. Since x is transcendental over k, this degree is ∞.

Assume now that at least one of n, m is nonzero: then z is transcendental over K (otherwise x would be algebraic over k), and let $L = k(z)$. It's immediate to see that $L(x) = k(x)$, so in order to compute the degree of the extension $L(x)/L$ we can try to find the minimal polynomial of x over L.

A natural candidate is $p(t) := zg(t) - f(t) \in L[t]$. The not-so-natural part consists in proving that p is irreducible in $L[t]$. Note that since f, g are coprime then p is primitive as a polynomial in $k[z][t]$. Hence by Gauss's lemma $p(t)$ is irreducible in $L[t]$ iff it's irreducible in $k[z, t]$ iff it's irreducible in $k(t)[z]$. But in this last ring, p has degree one as a polynomial in z, hence it's irreducible. Awesome! We found the minimal polynomial of x over L. It's easy to see that its degree (in t) is the maximum of n, m. Therefore, if $z \notin k$,

$$[k(x) : k(z)] = \max\{\deg g, \deg f\}$$

$\blacksquare$

8. Let $\alpha = \frac{1+\sqrt{5}}{2}$ denote the Golden Ratio. You are used to writing number to base 10, or other integer bases. This problem is about base α. Let $a_n, a_{n-1}, a_{n-2} \ldots$ be an infinite sequence of numbers in $\{0, 1\}$ with the property that $a_i a_{i+1}$ is never equal to 11. We will write

$$\beta = a_n \ldots a_1 a_0 \bullet a_{-1} a_{-2} \ldots$$

for

$$\beta = \sum_{j=-n}^{\infty} a_{-j} \alpha^{-j}$$

and call this the α-expansion for β.

1. Find the α-expansions for $2, 3, 4, 5$.
2. What is the number with α-expansion $0.101010\ldots$?
3. What is the number with α-expansion $0.100100100\ldots$?

Note that $\alpha^2 = \alpha + 1$. By induction, we see that $\alpha^n = F_n \alpha + F_{n-1}$ where F_n are the Fibonacci numbers.

1. Since $2 = \alpha + \alpha^{-2}$, we have $2 = 10 \cdot 01$. Adding $1 = \alpha^2 - \alpha$ shows $3 = \alpha^2 + \alpha^{-2} = 100 \cdot 01$. Incrementing gives $4 = 101 \cdot 01$. To represent 5 is a little harder, but if we calculate

$$\alpha^3 + \alpha^{-1} + \alpha^{-4} = 2\alpha + 1 + \alpha^{-1} + \alpha^{-4} = 3\alpha + (5 - 3\alpha) = 5$$

so $5 = 1000 \cdot 1001$.

2. Let S be the mystery number. Then

$$\alpha S = \sum_{n=0}^{\infty} \alpha^{-2n} = \frac{1}{1 - \alpha^{-2}}$$

Hence, $S = \frac{1}{\alpha - \alpha^{-1}} = 1$.

3. Let T be the mystery number. Then

$$\alpha T = \sum_{n=0}^{\infty} \alpha^{-3n} = \frac{1}{1 - \alpha^{-3}}$$

Hence,

$$T = \frac{1}{\alpha - \alpha^{-2}} = \frac{1}{\alpha - (2 - \alpha)} = \frac{\alpha}{2} = \frac{1 + \sqrt{5}}{4}$$

since $2\alpha(\alpha - 1) = 2$

■

9. Let $\omega = e^{\frac{2\pi i}{5}}$. Find the minimal polynomial for $\psi := \omega^2 + \omega^3$ over $\mathbb{Q}$ and the degree of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$.

Since $\omega^5 - 1 = 0$ and $\omega \neq 1$ then $1 + \omega + \ldots + \omega^4 = 0$. Then it's quite easy to check that

$$\psi^2 + \psi - 1 = 0$$

so ψ is a root of $p(x) := x^2 + x - 1$. Since p is irreducible over the rationals (there are no roots in $\mathbb{Q}$) then it's the minimal polynomial for ψ. ∎

10. A complex number is algebraic if it is the root of an irreducible polynomial with coefficients in $\mathbb{Q}$. If α and β are algebraic, show that $\alpha + \beta$ and $\alpha\beta$ are also algebraic.

We'll use repeatedly the fact that the simple extension $k(\xi)/k$ is algebraic iff it's finite.

Since α is algebraic over $\mathbb{Q}$, then it's also algebraic over $\mathbb{Q}(\beta)$: indeed, if $p(\alpha) = 0$ for some irreducible p in $\mathbb{Q}$, then $p'(\alpha) = 0$ for some irreducible factor of p in $\mathbb{Q}(\beta)[x]$. In particular, $\mathbb{Q}(\beta)(\alpha)/\mathbb{Q}(\beta)$ is a finite extension.

Consider now the extension $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$: we have that

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

and since the factors on the right hand side are finite, the extension $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ is finite, hence algebraic.

Since both $\alpha + \beta$, and $\alpha\beta$ lie in $\mathbb{Q}(\alpha, \beta)$, then they're algebraic. ∎