Math 641 Final Exam Solutions Fall 2012

1. **Solution:** Let

$$M = \{f(u)g(u)^{-1} : f(x) \in K[x],\ g(x) \in K[x],\ g(u) \neq 0\}.$$

Since each $f(u)$ and $g(u)$ belongs to F by closure of addition and multiplication in F, $M \subseteq F$. It clearly contains K and u. It is a field: it is easy to demonstrate that M is closed with respect to addition and multiplication, contains an additive and a multiplicative identity, and contains additive and multiplicative inverses. Since L is the intersection of all fields in F containing K and u, it is a subset of each, so it is a subset of M. Since L is a field containing both K and u, by closure of addition and multiplication it must contain all the expressions in M. Hence $M \subseteq L$. Therefore $L = M$.

2. **Solution:** Let

$$M = \{f(u)g(u)^{-1} : f(x) \in K[x],\ g(x) \in K[x],\ g(u) \neq 0\}.$$

M is a subring of F that contains both K and u. We must show that it is a field. Let $f(x) \in K[x]$ be given such that $f(u) \neq 0$. We will show that $f(u)$ has a multiplicative inverse in M. Let $p(x) = \text{irr}_K(u)$. Let $d(x)$ be the monic polynomial of least degree in the set

$$S = \{a(x)p(x) + b(x)f(x) : a(x), b(x) \in K[x]\}.$$

We showed earlier in the course that $d(x)|p(x)$ and $d(x)|f(x)$ by a division algorithm argument. Since $d(x)$ and $p(x)$ are both monic and $p(x)$ is irreducible, we must have $d(x) = 1$ or $d(x) = p(x)$. The latter case is ruled out because $p(x)$ cannot divide $f(x)$ by virtue of $p(u) = 0$ and $f(u) \neq 0$. Therefore $d(x) = 1$ and there are polynomials $a(x)$ and $b(x)$ in $K[x]$ such that $a(x)p(x) + b(x)f(x) = 1$. Evaluating at u we obtain $b(u)f(u) = 1$. Therefore $f(u)^{-1} = b(u) \in M$. Now that we know that M is a field, we must have $L \subseteq M$ since L is a subset of every field containing both K and u. Since L contains both K and u, it contains all the expressions in M by closure of addition and multiplication in L. Therefore $M \subseteq L$. Hence $L = M$.

An alternative solution is to show that $M \cong K[x]/(p(x))$. The quotient ring is a field since $(p(x))$ is maximal by virtue of the fact that $p(x)$ is irreducible. Since M is isomorphic to a field, it is a field. But I like the direct construction of the inverse above.

3. **Solution:** $s = (2^{1/3}\xi, \xi)$, $t = (2^{1/3}, \xi^2)$ satisfies $o(s) = 3$, $o(t) = 2$, $ts = s^2t = (2^{1/3}\xi^2, \xi^2)$.

4. **Solution:** A Mathematica calculation (see the notebook online) yields

$$p(x) = 127 + 123x + 6x^2 - 29x^3 - 6x^4 + 3x^5 + x^6.$$

We argue that this polynomial is irreducible. Reason: if $\mathrm{irr}_{\mathbb{Q}}(u)$ has degree less than 6 then $[\mathbb{Q}[u] : \mathbb{Q}] < 6$, therefore $\mathbb{Q}[u]$ is equal to one of the proper intermediate fields in the splitting field extension $\mathbb{Q} \subseteq \mathbb{Q}[2^{1/3}, \xi]$ which we calculated in the Galois Correspondence handout. This forces u to belong to one of these. But it doesn't (proof below). Therefore $\mathrm{irr}_{\mathbb{Q}}(u)$ has degree 6. Since it is a divisor of $p(x)$, it is equal to $p(x)$.

$u \notin \mathbb{Q}$: Because u is not a real number.

$u \notin \mathbb{Q}[2^{1/3}]$: Because u is not a real number.

$u \notin \mathbb{Q}[\xi]$: If $u = a + b\xi + c\xi^2$ then

$$2^{1/3} + 2^{2/3} + \xi - a + b\xi + c\xi^2 = 0.$$

Applying complex conjugation to this,

$$2^{1/3} + 2^{2/3} + \xi^2 - a + b\xi^2 + c\xi = 0.$$

Adding, and using $\xi + \xi^2 = -1$, we obtain

$$22^{1/3} + 22^{2/3} - 1 - 2a - b - c = 0.$$

In other words,

$$(-1 - 2a - b - c)1 + 22^{1/3} + 22^{2/3} = 0,$$

which contradicts the fact that $1, 2^{1/3}, 2^{2/3}$ are linearly independent as basis elements of $\mathbb{Q}[2^{1/3}]$.

$u \notin \mathbb{Q}[2^{1/3}\xi]$: If $u = a + b2^{1/3}\xi + c2^{2/3}\xi^2$ then

$$2^{1/3} + 2^{2/3} + \xi - a - b2^{1/3}\xi - c2^{2/3}\xi^2 = 0.$$

Substituting $\xi^2 = -1 - \xi$ and rearranging slightly, we obtain

$$(2^{1/3} + (1 + c)2^{2/3} - a) + \xi(1 - b2^{1/3} + c2^{2/3}) = 0.$$

Since ξ is not a real number we must have $1 - b2^{1/3} + c^{2/3} = 0$. However, the latter equation contradicts the fact that $1, 2^{1/3}, 2^{2/3}$ are linearly independent as basis elements of $\mathbb{Q}[2^{1/3}]$.

5. **Solution:** (a) $\mathbb{Q}[3^{1/4}, i] = \mathbb{Q}[3^{1/4}, -3^{1/4}, 3^{1/4}i, -3^{1/4}] = \mathbb{Q}[\text{roots of } x^4 - 3]$.

(b) First we compute the Galois Group. $\text{irr}_{\mathbb{Q}}(3^{1/4}) = x^4 - 3$, so valid images of $3^{1/4}$ are $3^{1/4}, -3^{1/4}, 3^{1/4}i, -3^{1/4}i$. $\text{irr}_{\mathbb{Q}[3^{1/4}]}(i) = x^2 + 1$, which is fixed under all priming operations, so valid images of i are roots of $x^2 + 1$, namely $i, -i$. So

$$\text{Gal}_{\mathbb{Q}}(\mathbb{Q}[3^{1/4}, i]) =$$
$$\{(3^{1/4}, i), (-3^{1/4}, i), (3^{1/4}i, i), (-3^{1/4}i, i),$$
$$(3^{1/4}, -i), (-3^{1/4}, -i), (3^{1/4}i, -i), (-3^{1/4}i, -i)\}.$$

See the scanned documents for the Galois Correspondence chart. The subfields $\mathbb{Q}[3^{1/4}, i]$, $\mathbb{Q}[3^{1/2}, i]$, $\mathbb{Q}[i]$, $\mathbb{Q}[3^{1/2}i]$, $\mathbb{Q}[3^{1/2}]$, and $\mathbb{Q}$ are all normal extensions of $\mathbb{Q}$ as splitting fields of $x^4 - 3$, $(x^2 + 3)(x^2 + 1)$, $x^2 + 1$, $x^2 + 3$, $x^2 - 3$, and $x - 1$, respectively. Since the polynomial $x^4 - 3$ is irreducible in $\mathbb{Q}[x]$ and has at least one but not all roots in both $\mathbb{Q}[3^{1/4}]$ and $\mathbb{Q}[3^{1/4}i]$, these two subfields are not normal extensions of $\mathbb{Q}$.

6. **Solution:** This is a nice illustration of Problem 2 of this exam. A Mathematica calculation (see the two notebooks online) yields

$$(a + b2^{1/3} + c2^{2/3})^{-1} = \frac{a^2 - 2bc}{d} + \frac{2c^2 - ab}{d}2^{1/3} + \frac{b^2 - ac}{d}2^{2/3}$$

where

$$d = a^3 + 2b^3 + 4c^3 - 6abc.$$

For example,

$$(1 + 2 \cdot 2^{1/3} + 3 \cdot 2^{2/3})^{-1} = \frac{-11}{89} + \frac{16}{89}2^{1/3} + \frac{1}{89}2^{2/3}.$$

Interestingly, our formula implies that the only rational solution to the equation $a^3 + 2b^3 + 4c^3 = 6abc$ is $a = b = c = 0$.