Solution to Homework 7. Math 113 Summer 2016.

1. Compute the minimal polynomials and find the degree of the following simple extensions of $\mathbb{Q}$:

   (a) $\mathbb{Q}(\sqrt{-3})$
   (b) $\mathbb{Q}(\sqrt{3}+i)$
   (c) $\mathbb{Q}(\sqrt{2}-\sqrt{10})$
   (d) $\mathbb{Q}(e^{2\pi i/p})$, for p an odd prime.

   Solution: Let f denote the minimal polynomial.

   (a) $f = x^2+3$, $[\mathbb{Q}(\sqrt{-3}):\mathbb{Q}] = 2$.
   (b) $f = x^4-4x^2+16$, $[\mathbb{Q}(\sqrt{3}+\sqrt{-1}):\mathbb{Q}] = 4$.
   (c) $f = x^4-24x^2+64$, $[\mathbb{Q}(\sqrt{2}-\sqrt{10}):\mathbb{Q}] = 4$.
   (d) $f = x^{p-1}+x^{p-2}+\ldots+x+1$, $[\mathbb{Q}(e^{2\pi\sqrt{-1}/p}):\mathbb{Q}] = p-1$.

2. Find a primitive element for each of the following extensions, then use this to find their minimal polynomial and degree:

   (a) $\mathbb{Q}(i,\sqrt{3})$
   (b) $\mathbb{Q}(\sqrt[4]{2},\sqrt{2})$
   (c) $\mathbb{Q}(\sqrt{2},\sqrt{10})$

   Solution: Let α be the primitive element, K the given field.

   (a) $\alpha = \sqrt{-1}+\sqrt{3}$: indeed, we have $\mathbb{Q}(\alpha)\subset K$ and, since $4\alpha^{-1} = \sqrt{3}-\sqrt{-1}$, we can show that $\frac{1}{2}(\alpha+4\alpha^{-1}) = \sqrt{3}\in\mathbb{Q}(\alpha)$ and $\frac{1}{2}(\alpha-4\alpha^{-1}) = \sqrt{-1}\in\mathbb{Q}(\alpha)$. Hence, $K\subset\mathbb{Q}(\alpha)$ and $K=\mathbb{Q}(\alpha)$. Moreover, the subset $\{1,\sqrt{3},\sqrt{-1},\sqrt{-3}\}$ is linearly independent over $\mathbb{Q}$: the set $\{1,\sqrt{3}\}$ is linearly independent over $\mathbb{Q}$ since $\sqrt{3}$ is irrational, hence the same is true of $\{\sqrt{-1},\sqrt{-3}\}$. As these two subsets are contained in different (real) lines in $\mathbb{C}$, then set $\{1,\sqrt{3},\sqrt{-1},\sqrt{-3}\}$ is linearly independent. Hence, $[K:\mathbb{Q}]\geq 4$. Since α is a root of $f = x^4-4x^2+16$, we see that $[K:\mathbb{Q}] = 4$ and f is the minimal polynomial.
   (b) Here you can actually just use $\sqrt[4]{2}$ as the primitive element. It generates $\sqrt{2}$ since $(\sqrt[4]{2})^2 = \sqrt{2}$.
   (c) $\sqrt{2}+\sqrt{10}$ is a primitive element. Argument similar to (a).

3. Prove that, up to isomorphism, there are no finite extensions of $\mathbb{C}$ except $\mathbb{C}$ itself. In other words, if L is a finite extension of $\mathbb{C}$, then $L\cong\mathbb{C}$. Does there exist an algebraic extension of $\mathbb{C}$? Explain your answer.

   Solution: Let L be a finite extension of $\mathbb{C}$. Then, L is simple, so that there is some $\alpha\in L$ such that $L=\mathbb{C}(\alpha)$. Let $f\in\mathbb{C}[x]$ be the minimal polynomial of α, so that $L\cong\mathbb{C}[x]/(f)$ and f is irreducible. By the Fundamental Theorem of Algebra, $\deg f = 1$, so that $f = x-a$. Then, $f(\alpha)=0 \implies a=\alpha \implies \alpha\in\mathbb{C}$. Hence, $L=\mathbb{C}(\alpha)=\mathbb{C}$ (here we identify $\mathbb{C}$ with its image in L). There does not exist a proper algebraic extension: if there did, call it F, then every element of F would algebraic over $\mathbb{C}$. This means that if $\alpha\in F$ then there is a minimal polynomial $f\in\mathbb{C}[x]$ such that $f(\alpha)=0$. But f, being the minimal polynomial, would also be irreducible, and the only irreducible polynomials over $\mathbb{C}$ are the linear ones, so $f = x-\alpha$ (up to units), hence, since $f\in\mathbb{C}[x]$, $\alpha\in\mathbb{C}$. Thus $F=\mathbb{C}$.

4. Let K be the field obtained by adjoining all three cube roots of 2 to $\mathbb{Q}$. Show that K contains all cube roots of unity and compute its degree over $\mathbb{Q}$. [Hint for the degree computation: you may want to let L be the field obtained by adjoining $\omega = \frac{-1+i\sqrt{3}}{2}$ to $\mathbb{Q}$, and factorize the extension as $\mathbb{Q} \subset L \subset K$. Note that $\omega^3 = 1$.]

   Solution: The three cube roots of 2 are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. Since K contains these, and is a field, it also contains $\omega = \omega^2\sqrt[3]{2}/\omega\sqrt[3]{2}$, and hence also ω^2. Obviously 1 is in $\mathbb{Q}$, so K contains all three of the cube rots of unity. So in fact we can write $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$. To find its degree factorize the extensions as $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset K$. We have seen that the degree of $\mathbb{Q}(\omega)$ over $\mathbb{Q}$ is 2 (its minimal polynomial is $x^2 + x + 1$). Since $K = \mathbb{Q}\omega)(\sqrt[3]{2})$,its minimal polynomial is just $x^3 - 2$ (but note that this is *not* the minimal polynomial of K over $\mathbb{Q}$, because $\sqrt[3]{2}$ is not a primitive element for K over $\mathbb{Q}$). Hence $[K : \mathbb{Q}(\omega)] = 3$, so since degree is multiplicative in towers, $[K : \mathbb{Q}] = 6$.

5. Suppose $f \in \mathbb{Q}[x]$, not necessarily irreducible.

   (a) Show that there is a smallest subfield of $\mathbb{C}$ over which f factors into linear factors. In other words, prove there exists a subfield K_f of $\mathbb{C}$ such that (i) f factors into linear factors in $K_f[x]$, and (ii) if L is any other subfield of $\mathbb{C}$ for which f factors into linear factors in $L[x]$, then $L \supseteq K_f$.

   (b) Taking $f = x^7 - x^4 - 4x^3 + 4$, find K_f by writing at as $\mathbb{Q}(\alpha, \beta, ...)$, and compute the degree of K_f over $\mathbb{Q}$.

   Solution:

   (a) Let $\{a_1, \dots, a_k\} \subset \mathbb{C}$ be the distinct roots of f. Then, $K_f = \mathbb{Q}(a_1, \dots, a_k)$. Obviously $f \in K_f[x]$ factors into linear factors; if L is a subfield such that $f \in L[x]$ factorises into linear factors then we must have $x - a_i \in L[x]$, for each i (since $\mathbb{C}[x]$ is a UFD and $L \subset \mathbb{C}$). Hence, we must have $a_i \in L$, for each i, so that $L \supset \mathbb{Q}(a_1, \dots, a_k)$, by definition.

   (b) We have

   $$x^7 - x^4 - 4x^3 + 4 = x^4(x^3 - 1) - 4(x^3 - 1) = (x^4 - 4)(x^3 - 1)$$

   and the last polynomial factorises as

   $$(x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{-2})(x + \sqrt{-2})(x - 1)(x - \omega)(x - \omega^2),$$

   where $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$. Hence, K_f is obtained by adjoining $\sqrt{2}, \sqrt{-1}, \sqrt{3}$. Adjoining each of these elements one at a time results in fields $\mathbb{Q} \subset E \subset F \subset K_f$, with each extension being of degree 2. Hence, $[K_f : \mathbb{Q}] = 8$.

6. Define $\mathcal{A} = \{\alpha \in \mathbb{C} \mid \text{there exists } f \in \mathbb{Q}[x] \text{ such that } f(\alpha) = 0\}$ - this is the set of **algebraic numbers**. For example, $\sqrt{2} \in \mathcal{A}$ (since $f(\sqrt{2}) = 0$, where $f = x^2 - 2$), and $\sqrt{-2} + \sqrt{3} \in \mathcal{A}$ (since $g(\sqrt{-2} + \sqrt{3}) = 0$, where $g = x^4 - 2x^2 + 25$).

   (a) Show that $\mathbb{Q} \subset \mathcal{A}$.

   (b) Let $\mathbb{Q} \subset L$ be an algebraic extension of $\mathbb{Q}$. Prove that $L \subset \mathcal{A}$.

   (c) Prove that $\mathcal{A}$ is a field. Deduce that it is the largest algebraic extension of $\mathbb{Q}$ in $\mathbb{C}$.

(d) Explain, using a single sentence, why $\mathcal{A} \neq \mathbb{C}$.[1]

Solution:

(a) If $a \in \mathbb{Q}$ it's algebraic because it's a root of the rational polynomial $x - a$.

(b) For any $a \in L$, a is algebraic over $\mathbb{Q}$ since L is an algebraic extension. But then a satisfies some polynomial f, so $a \in \mathcal{A}$.

(c) We need to show that $\mathcal{A}$ contains $0, 1$, and is closed under addition, multiplication and taking additive and multiplicative inverses. 0 and 1 are in $\mathcal{A}$ because they are roots of the rational polynomials x and $x - 1$, respectively. Now let $a, b \in \mathcal{A}$, both nonzero, and consider the extension $\mathbb{Q} \subset \mathbb{Q}(a, b)$. It's finite because it factors as $\mathbb{Q} \subset \mathbb{Q}(a) \subset \mathbb{Q}(a, b)$, both of which are simple extensions by a and b, and since a and b are algebraic, these are simple algebraic extensions. But being finite over $\mathbb{Q}$, $\mathbb{Q}(a, b)$ is also algebraic over $\mathbb{Q}$, and so any element of $\mathbb{Q}(a, b)$ is algebraic over $\mathbb{Q}$. In particular, $a + b, ab, -a$, and a^{-1} are all algebraic over $\mathbb{Q}$, and hence in $\mathcal{A}$.

(d) $\pi \in \mathbb{C}$ but π is not algebraic over $\mathbb{Q}$.

7. Let $K = \mathbb{Q}(i\sqrt[4]{2})$ and $L = \mathbb{Q}(i\sqrt[4]{2}, \sqrt{3})$, so that $\mathbb{Q} \subset K \subset L$.

(a) Give an example of an embedding of K which is not an automorphism.

(b) Give an example of an automorphism of L which does not fix K pointwise.

Solution:

(a) Consider the homomorphism f defined by mapping $i\sqrt[4]{2} \mapsto \sqrt[4]{2}$ - this defines an embedding that is not an automorphism, since im $f \subset \mathbb{R}$ and $\mathbb{Q}(i\sqrt[4]{2}) \not\subset \mathbb{R}$.

(b) You can consider the automorphism g such that $g(i\sqrt[4]{2}) = -i\sqrt[4]{2}, g(\sqrt{3}) = \sqrt{3}$. This does not fix K pointwise.

8. Consider the extension $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

(a) Prove that every automorphism of $\mathbb{Q}(\sqrt[4]{2})$ fixes $\mathbb{Q}(\sqrt{2})$ pointwise.

(b) Deduce that $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})) = \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$.

(c) Show that $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ is a normal extension, but $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ is not.

(d) Using (b), or otherwise, compute $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$.

Solution:

(a) The minimal polynomial of $\sqrt[4]{2}$ is $x^4 - 2$, and its roots are $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. So any automorphism of $\mathbb{Q}(\sqrt[4]{2})$ must send $\sqrt[4]{2}$ to one of these roots, but only the first two live in $\mathbb{Q}(\sqrt[4]{2})$. So the only automorphisms of $\mathbb{Q}(\sqrt[4]{2})$ send $\sqrt[4]{2}$ to $\pm\sqrt[4]{2}$, and both of these send $\sqrt{2} = (\sqrt[4]{2})^2$ to $(\pm\sqrt[4]{2})^2 = \sqrt{2}$.

(b) This follows immediately from (a): there are the same two automorphisms in each Galois group.

(c) The first extension is normal because its Galois group has size two (by the argument in (a)), and its degree is also two. The second is not because its Galois group has size two (by the argument in (a)) but it is a degree four extension.

[1] In fact, the algebraic integers are **countable**: this means that there is a bijection $\{1, 2, 3, ...\} \leftrightarrow \mathcal{A}$. The real numbers are **uncountable** so that there is no bijection $\{1, 2, 3, \dots, \} \leftrightarrow \mathbb{R}$; this means that there are *many* more real numbers than algebraic integers.

(d) The two automorphisms in $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$ are the identity map and the map determined by mapping $\sqrt[4]{2}$ to $-\sqrt[4]{2}$.

9. Compute the Galois group of $\mathbb{Q} \subset \mathbb{Q}(i + \sqrt{2})$. List all intermediate subfields of the extension.

Solution: We have seen in class that $\mathbb{Q}(i + \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$, so any automorphism of $\mathbb{Q}(i, \sqrt{2})$ is determined by what it does to i and $\sqrt{3}$ - there are four possibilities $g_{++}, g_{-+}, g_{+-}, g_{--}$, where $g_{-+}(i) = -i, g_{-+}(\sqrt{3}) = \sqrt{3}$ etc. Each of these automorphisms has order two so that $\mathrm{Gal}(\mathbb{Q}(i + \sqrt{2}), \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the Klein four group. Since the extension is normal - $[\mathbb{Q}(i + \sqrt{2}) : \mathbb{Q}] = 4 = |\mathrm{Gal}(\mathbb{Q}(i + \sqrt{2}) : \mathbb{Q})|$ - the Galois connection is a bijection, so there are five intermediate subfields $\mathbb{Q}, \mathbb{Q}(i + \sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2})$, corresponding respectively to the subgroups $\mathrm{Gal}(\mathbb{Q}(i + \sqrt{2}), \mathbb{Q}), \{\mathrm{id}\}, \langle g_{++} \rangle, \langle g_{+-} \rangle, \langle g_{-+} \rangle, \langle g_{--} \rangle$.

10. Compute the Galois group of $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$.

Solution: An automorphism is determined by its effect on $\sqrt[3]{2}$ and $i\sqrt{3}$. The first must map to one of $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ and $i\sqrt{3}$ must map to one of $\{\pm i\sqrt{3}\}$. Notice that since $\omega = \frac{-1+i\sqrt{3}}{2}$, negating $i\sqrt{3}$ has the effect of sending ω to $\omega^2 = \overline{\omega}$. Moreover this extension is normal, since the conjugates of both generators all live in the field. So there will be six automorphisms, and we can write them all down by listing all "permutations of the roots" of the minimal polynomials for each generator. We get

$$\sigma_1 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ i\sqrt{3} \mapsto i\sqrt{3} \end{cases} \quad \sigma_2 : \begin{cases} \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \\ i \mapsto i\sqrt{3} \end{cases} \quad \sigma_3 : \begin{cases} \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \\ i \mapsto i\sqrt{3} \end{cases}$$

$$\sigma_4 : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ i \mapsto -i\sqrt{3} \end{cases} \quad \sigma_5 : \begin{cases} \sqrt[3]{2} \mapsto \omega\sqrt[3]{2} \\ i \mapsto -i\sqrt{3} \end{cases} \quad \sigma_6 : \begin{cases} \sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2} \\ i \mapsto -i\sqrt{3} \end{cases}$$

Now this group, being of order six, must be isomorphic to either $\mathbb{Z}/6\mathbb{Z}$ or S_3, as we saw in the group theory part of the course. We claim it's isomorphic to S_3, and can show this by verifying that it's not abelian - for instance, σ_2 and σ_4 do not commute. To see this, let's calculate the effect of both $\sigma_2\sigma_4$ and $\sigma_4\sigma_2$ on the element $\sqrt[3]{2}$:

$$\sigma_2\sigma_4(\sqrt[3]{2}) = \sigma_2(\sqrt[3]{2}) = \omega\sqrt[3]{2},$$

whereas

$$\sigma_4\sigma_2(\sqrt[3]{2}) = \sigma_4(\omega\sqrt[3]{2}) = \sigma_4(\omega)\sigma_4(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}.$$

Thus $\sigma_2\sigma_4$ and $\sigma_4\sigma_2$ are not the same function, so this group of automorphisms is not abelian.